Better Every Day

PROTECTION OF PERSONAL INFORMATION (POPI ACT)

Montego
Pet Nutrition

Contents

1. INTRODUCTION

This Policy, of utmost importance, outlines the obligations of Montego Pet Nutrition, a company registered in South Africa under number 4680187368, whose registered office is at 2 Bresler Street, Graaf Reinet, 6280 ("the Company"), regarding the protection of personal information and the rights of employees, customers, business contacts, etc. ("data subjects") in respect of their personal information under The Protection of Personal Information Act or "POPIA". "The Protection of Personal Information Act" refers to the legislation and regulations in force from time to time that regulate the use of personal information.

This Policy outlines the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal information. The procedures and principles outlined herein must be followed by the Company, its employees, agents, contractors, and other parties working on behalf of the Company.

2. SCOPE

The Company is committed to the letter and spirit of the law. It places high importance on the correct, lawful, and fair handling of all personal information and respects the legal rights, privacy, and trust of all individuals with whom it deals.

The HR Officer is responsible for administering this Policy and developing and implementing applicable policies, procedures, and/or guidelines.

The Company's HR Officers will assist him/her with ensuring compliance with the Protection of Personal Information Act. The Human Resources Department maintains the most up-to-date information on the HR Officers.

All employees appointed in positions with an inherent function of supervising others and/or performing a department/division/unit are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

- Any questions relating to this Policy or POPIA should be referred to the HR Office. In particular, the HR Officers or HR Manager should always be consulted in the following cases:
- if there is any uncertainty relating to the lawful basis on which personal information will be collected, held, and/or processed.
- if consent is not being relied upon to collect, hold, and/or process personal information.
- if there is any uncertainty relating to the retention period for any particular type(s) of personal information.
- if any new or amended Privacy Notices or similar privacy-related documentation are required.
- if any assistance is required in exercising a data subject's rights (including, but not limited to, handling data subject access requests).
- if a personal information breach (suspected or actual) has occurred.

- if there is any uncertainty about the security measures (whether technical or organisational) required to protect personal information.
- if personal information is to be shared with third parties (whether such third parties act as third-party service providers or operators).
- If personal information is to be transferred outside of South Africa, there are questions relating to the legal basis on which to do so and legislation, binding corporate rules, or agreements that protect such personal information in third-party countries.
- A POPIA Impact Assessment is required when a significant new processing activity is to be carried out or important changes are to be made to existing processing activities.
- when personal information is to be used for purposes different to those for which it was initially collected.
- if any automated processing, including profiling or automated decision-making, is to be carried out or
- If any assistance is required to comply with the law applicable to direct marketing using electronic communication.

3. DEFINITIONS

Term	Definition
Consent	Any voluntary, specific, and informed expression of will in terms of which permission is given to the processing of personal information;
Responsible party	The natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of processing personal information. For this Policy, the Company is the responsible party for all personal information relating to data subjects, such as employees, customers, and business contacts, used in our business for commercial purposes.
Operator	A natural or legal person or organisation which processes personal information on behalf of a responsible party;
Data subject	A living, identifiable natural person or existing juristic person about whom the Company holds personal information;
Personal Information	Any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to– This means any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to– (a) information relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-

	being, disability, religion, conscience, belief, culture, language, and the person's birth. (b) information about the person's education, medical, financial, criminal, or employment history. (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person. (d) the biometric information of the person. (e) the personal opinions, views, or preferences of the person. (f) correspondence sent by the person that is implicitly or explicitly private or confidential nature, or further correspondence that would reveal the contents of the original correspondence. (g) the views or opinions of another individual about the person and (h) 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
Personal information breach	A breach of security leading to the accidental or unlawful disclosure of, access to, or use of personal information under the control of the Company;
Processing	Any operation or set of operations performed on personal information or sets of personal data, whether or not by automated means, such as but not limited to the collection, receipt, recording, organisation, structuring, storage, adaptation/alteration, retrieval, use, disclosure by transmission/dissemination or otherwise making available, alignment, merging, linking/combining, restriction, erasure or destruction thereof.
De-identify	To delete any information that– (a) identifies the data subject. (b) can be used or manipulated by a reasonably foreseeable method to determine the data subject, or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.
Special personal information	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 (b) the criminal behaviour of a data subject to the extent that such information relates to–

	(i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject to the disposal of such proceedings.

4. THE PROTECTION OF PERSONAL INFORMATION PRINCIPLES

This Policy aims to ensure compliance with POPIA and sets out the following principles that any party handling personal information must comply with. Responsible Parties are responsible for and must be able to demonstrate such compliance. All personal data must be:

- Process lawfully, fairly, and transparently about the data subject.
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, for historical, research, or statistical purposes, shall not be considered incompatible with the initial purposes.
- adequate, relevant, and limited to what is necessary about the purposes for which it is processed.
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal information regarding the purposes for which it is processed is erased/destroyed, or rectified without delay.
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed. Personal information may be stored for extended periods as long as it is processed solely for archiving purposes in the public interest, such as for historical, statistical, or research purposes, subject to the implementation of appropriate safeguards to prevent such records from being used for any other purpose.
- processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. THE RIGHTS OF DATA SUBJECTS

POPIA sets out the following fundamental rights applicable to data subjects:

- The right to be informed.
- the right of access.
- the right to rectification.
- the right to erasure (the 'right to be forgotten').
- the right to restrict processing.
- the right to object; and
- rights concerning automated decision-making and profiling.
- rights concerning direct marketing using electronic communication as a medium.

6. LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

POPIA ensures that personal information is processed lawfully without adversely affecting the data subject's rights. Specifically, the processing of personal information shall be lawful if at least one of the following applies:

- The data subject has given consent to process their personal information for one or more specific purposes.
- the processing is necessary to perform a contract to which the data subject is a party or to take steps at the data subject's request before agreeing.
- the processing is necessary for compliance with a legal obligation to which the responsible party is subject.
- the processing is necessary to protect the legitimate interests of either the data subject, the responsible party or a third party to whom such information is supplied or
- the processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the responsible party, or
- If the personal information in question is a particular category of personal data (also known as "special personal information"), at least one of the following conditions must be met:
- The data subject has given explicit consent to process such data for one or more specified purposes (unless the law prohibits them from doing so).
- the processing is necessary to establish, exercise, or defend a right or obligation in law.
- processing is required to serve an obligation in public or international law.
- The processing relates to personal information deliberately made public by the data subject.
- The processing is necessary for the conduct of legal claims or when courts act in their judicial capacity.
- the Information Regulator authorises the processing upon successful application or
- the processing is necessary for archiving purposes in the public interest for historical, research or statistical purposes.

7. CONSENT

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal information, the following shall apply:

- Consent is a clear indication, as far as possible in writing, by the data subject that they agree to process their personal information. Silence, pre-ticked boxes, or inactivity do not amount to consent.
- Where consent is given in a document which includes other matters, the section dealing with consent must be kept separate from such other issues.

- Data subjects are free to withdraw consent at any time, and it must be accessible for them to do so. If a data subject withdraws their consent, the request must be honoured promptly, unless such withdrawal would significantly adversely affect the responsible party.
- If personal information is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal information was initially collected, that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
- If particular personal information is processed, the Company shall generally rely on a lawful basis other than explicit consent. However, if explicit consent is relied upon, the data subject must do so in writing.
- In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal information, records must be kept of all consents obtained to ensure that the Company can comply with consent requirements.

8. SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES

The Company collects and processes the personal information set out in Part 23 of this Policy. This includes:

- personal information collected directly from data subjects or
- personal information obtained from third parties.
- The Company only collects, processes, and holds personal information for the specific purposes set out in Part 23 of this Policy (or other purposes expressly permitted by POPIA).
- Data subjects must always be informed of the purpose or purposes for which the Company uses their personal information. Please refer to Part 15 for more information on keeping data subjects informed.

9. ADEQUATE, RELEVANT, AND LIMITED PROCESSING

The Company will only collect and process personal information for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 23, below.

- Employees, agents, contractors, or other parties working on behalf of the Company may collect personal information only to the extent required to perform their job duties and only in accordance with this Policy. Excessive personal data must not be collected.
- Employees, agents, contractors, or other parties working on behalf of the Company may process personal information only when performing their job duties require it. The Company does not process personal data for unrelated purposes.

10. ACCURACY OF PERSONAL INFORMATION / KEEPING UP TO DATE

The Company shall ensure that all personal information it collects, processes, and holds is accurate and up-to-date. This includes, but is not limited to, rectifying personal information at the request of a data subject, as outlined in Part 17 below.

The accuracy of personal information shall be checked when it is collected and, as determined by each Departmental Head, as and when required, due to the nature and purpose of the personal information.

If any personal information is inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data as appropriate.

11. RETENTION OF PERSONAL INFORMATION

The Company shall not keep personal information for any longer than is necessary in light of the purpose or purposes for which that personal information was initially collected, held, and processed.

When personal information is no longer required, all reasonable steps will be taken to erase or dispose of it immediately.

.

12. SECURE PROCESSING

The Company shall ensure that all personal information collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and accidental loss, destruction, or damage. Parts 25 to 30 of this Policy provide further details of the technical and organisational measures to be taken.

All technical and organisational measures to protect personal information shall be reviewed and evaluated to ensure their ongoing effectiveness and personal data security.

Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal information as follows:

- only those with a genuine need to access and use personal information and who are authorised may access and use it.
- personal information must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
- Authorised users must always be able to access personal information as required for authorised purposes.

13. ACCOUNTABILITY AND RECORD-KEEPING

The HR Officer is responsible for administering this Policy and developing and implementing applicable policies, procedures, and/or guidelines.

- The Company shall always follow a "privacy by design" approach when collecting, holding, and processing personal information.
- All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in protecting personal information, addressing the relevant aspects of POPIA, this Policy, and all other applicable Company policies.

- The Company's protection of personal information compliance shall be regularly reviewed and evaluated using POPIA Audits.
- The Company shall keep written internal records of all personal information collection, holding, and processing, which shall incorporate the following information:
- the Company's name and details, and any applicable operators with whom personal information is shared.
- the purposes for which the Company collects, holds, and processes personal information.
- the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such permission, and records of such authorisation) for collecting, holding, and processing personal information.
- details of the categories of personal information collected, held, and processed by the Company.
- details of any transfers of personal information outside of South Africa, including security safeguards.
- The Company will retain details of how long personal information is retained.
    - details of personal information storage, including location(s).
    - detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal information.

14. KEEPING DATA SUBJECTS INFORMED

The Company shall provide the information set out in Part 15.2 to every data subject:

- where personal information is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection and
- where personal information is obtained from a third party, the relevant data subjects will be informed of its purpose:
- if the personal information is used to communicate with the data subject when the first communication is made, or
- if the personal information is to be transferred to another party before that transfer is made or
- as soon as reasonably possible and preferably not more than one month after obtaining personal information.

The following information shall be provided in the form of a privacy notice:

- Company details include, but are not limited to, contact details and the names and contact details of any applicable representatives and HR Officers.
- the purpose(s) for which the personal information is being collected and will be processed (as detailed in Part 23 of this Policy).
- where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal information.
- where the personal information is to be transferred to a third party outside of South Africa, details of that transfer, including but not limited to the safeguards in place (see Part 30 of this Policy for further information).
- Details of the data subjects' rights under POPIA.
- details of the data subject's right to withdraw their consent to the Company's processing of their personal information at any time.
- details of the data subject's right to complain to the Information Regulator.

- details of any automated decision-making or profiling that will take place using personal information, including information on how decisions will be made, the significance of those decisions, and any consequences.

15. DATA SUBJECT ACCESS

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal information that the Company holds about them, what it is doing with that personal information, and why.

Data subjects wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the Company's HR Officers.

- Responses to SARs must usually be made within one month of receipt. However, this may be extended by up to two months if the SAR is complex and numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the Company's HR Officers and the Company's Data Subject Access Request Policy and procedure.
- The Company may charge a reasonable fee for handling normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information already supplied to a data subject and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. RECTIFICATION OF PERSONAL INFORMATION

Data subjects have the right to require the Company to rectify any inaccurate or incomplete personal information.

- The Company shall rectify the personal information in question and inform the data subject of that rectification within one month of the data subject reporting the Company of the issue. The period can be extended by up to two months for complex requests. If such additional time is required, the data subject shall be informed.
- The Company may decline a data subject's request for personal information to be corrected and will keep a record of such request and the basis for denying the application.

17. ERASURE OF PERSONAL INFORMATION

Data subjects have the right to request that the Company erase the personal information it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal information concerning the purpose(s) for which it was initially collected or processed.
- The data subject wishes to withdraw their consent to the Company's holding and processing of their personal information.
- the data subject objects to the Company holding and processing their personal information (and there is no overriding legitimate interest to allow the Company

to continue doing so) (see Part 20 of this Policy for further details concerning the right to object).

- The personal information was processed unlawfully.
- the personal information must be erased for the Company to comply with a particular legal obligation.

Unless the Company has reasonable grounds to refuse to erase personal information, all requests for erasure shall be complied with, and the data subject shall be informed of the erasure within one month of receipt of the data subject's request. The period can be extended by up to two months for complex requests. If such additional time is required, the data subject shall be informed.

18. RESTRICTION OF PERSONAL INFORMATION PROCESSING

Data subjects may request that the Company cease processing their personal information. Suppose a data subject makes such a request. In that case, the Company shall retain only the personal information concerning that data subject (if any) necessary to ensure that the personal information in question is not processed further.

19. OBJECTIONS TO PERSONAL INFORMATION PROCESSING

Data subjects have the right to object to the Company processing their personal information based on legitimate interests or for direct marketing.

- Where a data subject objects to the Company processing their personal information based on its legitimate interests, the Company shall cease such processing immediately unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
- Where a data subject objects to the Company processing their personal information for direct marketing purposes, the Company shall cease such processing promptly.

20. AUTOMATION

The Company does not use personal information in automated decision-making processes.

21. DIRECT MARKETING

The Company is subject to specific rules and regulations when marketing its products and/or services.

- The prior consent of data subjects is required for electronic direct marketing, including email, text messaging, and automated telephone calls, subject to the following limited exceptions:

- The Company may send marketing text messages or emails to a customer provided that the customer's contact details have been obtained during a sale, the marketing relates to similar products or services, and the customer in question has permitted the Company to do so. Furthermore, the customer can opt out of marketing communications from the Company in every subsequent communication.
- Direct marketing to data subjects, except as provided for in Part 22.2(a) above, may only occur upon being presented with written consent from the subject. The Direct Marketing Consent Form is to be used for this purpose.
- The right to object to direct marketing shall be offered to data subjects clearly and intelligibly. It must be kept separate from other information to preserve its clarity.
- If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal information may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

22. PERSONAL INFORMATION COLLECTED, HELD, AND PROCESSED

The Company shall ensure that the following measures are taken concerning the collection, holding, and processing of personal information:

- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of their responsibilities and the Company's responsibilities under the Protection of Personal Information Act and this Policy. They shall be provided with a copy of this Policy.
- Only employees, agents, contractors, or other parties working on behalf of the Company that need access to and use personal information to carry out their assigned duties correctly shall have access to personal data held by the Company.
- All sharing of personal information shall comply with the information provided to the relevant data subjects, and if required, the consent of such data subjects shall be obtained before sharing their personal information.
- All employees, agents, contractors, or other parties handling personal information on behalf of the Company will be appropriately supervised.
- All employees, agents, contractors, or other parties handling personal information working on behalf of the Company shall be encouraged to exercise care, caution, and discretion when discussing work-related matters related to personal data, whether in the workplace or otherwise.
- Methods of collecting, holding, and processing personal information shall be regularly evaluated and reviewed.
- The Company's Personal Information Retention Policy sets out a periodic review of all personal information held by the Company.
- The performance of employees, agents, contractors, or other parties handling personal information on behalf of the Company shall be regularly evaluated and reviewed.

- All employees, agents, contractors, or other parties handling personal information working on behalf of the Company will be bound to do so by the principles of POPIA and this Policy by contract.
- All agents, contractors, or other parties handling personal information on behalf of the Company must ensure that any of their employees involved in processing personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and POPIA.
- Where any agent, contractor, or other party handling personal information on behalf of the Company fails in their obligations under this Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims, or proceedings that may arise out of that failure.

22.1 TRANSFERRING PERSONAL INFORMATION INTERNATIONALLY

The Company may occasionally transfer ('transfer' includes making personal information available remotely) to countries outside South Africa. POPIA restricts such transfers to ensure that the protection given to data subjects is not compromised.

- Personal information may only be transferred to a country outside South Africa if one of the following applies:
- the personal information transferred to another country is protected by appropriate legislation; or
- adequate safeguards are in place, including binding corporate rules or
- a binding agreement is concluded between the Company and a third party that offers adequate protection or
- the transfer is made with the informed and explicit consent of the relevant data subject(s) or
- the transfer is necessary for the performance of a contract between the data subject and the Company or
- for the establishment, exercise, or defence of legal claims; or
- for the benefit of the data subject, where it is not reasonably practicable to obtain consent from the subject, and the subject would most likely not have objected.
- or the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

22.2 DATA BREACH NOTIFICATION

All personal information breaches must be reported immediately to the Company's HR Office.

- If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal information breach has occurred, they must not attempt to investigate it themselves. Any evidence relating to the personal information breach should be carefully retained.

- If a personal information breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the HR Manager must ensure that the Information Regulator's Office, as well as the data subject(s), are in writing informed of the breach without delay after having become aware of it unless such disclosure will interfere with a criminal investigation.
- Data breach notifications shall include the following information:
    - The categories and approximate number of data subjects concerned.
    - The categories and approximate number of personal information records concerned.
    - The name and contact details of the Company's HR Manager (or other contact point where more information can be obtained).
    - The likely consequences of the breach.
    - Details of the measures taken, or proposed to be taken, by the Company to address the breach, including, where appropriate, measures to mitigate its possible adverse effects and to prevent it from reoccurring.

22.3 EMPLOYEE PERSONAL INFORMATION

The Company holds a range of personal information about its employees. Employee personal information shall be collected, held, and processed according to employee data subjects' rights and the Company's obligations under the Protection of Personal Information Act and in accordance with this Policy. The Company may collect, hold, and process the employee's personal information, detailed in this Policy, but not limited to:

Identification and other information relating to employees:

- Name and surname.
- Contact Details.
- Addresses.
- Identification documentation.
- Work permits.
- Bank details.
- Next of kin information.
- Vehicle details (if applicable).
- Fingerprint / retinal images or voice samples for workplace access and company equipment use.

22.4 EMPLOYMENT EQUITY MONITORING

- Age.
- Gender.
- Ethnicity.
- Nationality.
- Culture.
- Health records (Please refer to Part 34, below, for further information):
- Details of sick leave.
- Medical conditions.

- Disabilities.
- Medical fitness reports.
- Employment records:
- Interview notes.
- CVs, application forms, cover letters, and similar documents.
- Assessments, performance reviews, and similar documents.
- Details of remuneration, including salaries, pay increases, bonuses, commission, overtime, benefits, and expenses.
- Details of trade union membership where applicable. Please refer to Part 36 below for further information.
- Employee monitoring information (please refer to Part 37 below).
- Records of disciplinary matters, including reports and warnings, both formal and informal.
- Details of grievances, including documentary evidence, interview notes, procedures followed, and outcomes.

22.5 BROAD-BASED BLACK ECONOMIC EMPOWERMENT

The Company may collect, hold, and process specific information for Employment Equity and Broad-Based Black Economic Empowerment purposes.

- Some of the personal information collected for this purpose, such as details of race, gender and disabilities, falls within POPIA's definition of particular personal information (see Part 2 of this Policy for a definition).
- Where possible, such particular personal information will be de-identified. Where unique personal information remains, it will be collected, held, and processed strictly in accordance with the conditions for processing specific personal data, as set out in Part 6.2 of this Policy.
- The Company's lawful basis for processing such data is found in the Employment Equity Act, the Broad-Based Black Economic Empowerment Act, and relevant regulations.
- Non-anonymised particular personal information under this part shall be accessible and used only by senior management and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company, except in exceptional circumstances where it is necessary to protect the legitimate interests of the employee data subject(s) concerned. Such circumstances satisfy one or more of the conditions in Part 6.2 of this Policy.

22.6 EMPLOYEE HEALTH RECORDS

- The Company holds health records on employee data subjects used to assess employees' health, well-being, and welfare and highlight any issues that may require further investigation. In particular, the Company prioritises maintaining health and safety in the workplace and preventing discrimination based on disability or other medical conditions.
- In most cases, health information on employees falls within POPIA's definition of particular personal information (see Part 2 of this Policy for a definition). Therefore, any data relating to the health of employee data subjects will be collected, held, and processed strictly in accordance with the conditions for

processing particular category personal information, as set out in Part 6.2 of this Policy.

- The Company's lawful basis for processing employees' health information is as provided for in relevant labour-related legislation, such as The Basic Conditions of Employment Act, The Mines Health and Safety Act, The Occupational Health and Safety Act, the Labour Relations Act, and the National Road Traffic Act.
- Health records shall be accessible and used only by the HR Department and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the Company without the express consent of the employee data subject(s) to whom such data relates, except in exceptional circumstances where it is necessary to protect the legitimate interests of the employee data subject(s) concerned. Such circumstances satisfy one or more of the conditions in Part 6.2 of this Policy.
- Health records will only be collected, held, and processed to the extent required to justify an employee's absence from work due to illness and to ensure that employees can perform their job correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

22.7 EMPLOYEE BENEFITS

- In cases where employee data subjects are enrolled in the Company's benefit schemes, third-party organisations may occasionally need to collect personal information from relevant employee data subjects.
- Before collecting such information, employee data subjects will be fully informed of the personal information to be gathered, the reasons for its collection, and how it will be processed, per the information requirements in Part 15 of this Policy.
- The Company shall not use any such personal information except as necessary in administering the relevant benefits schemes.

22.8 EMPLOYEE TRADE UNION MEMBERSHIP

The Company will provide the following personal information concerning relevant employee data subjects to trade unions registered by the Registrar of Labour Relations (Department of Employment and Labour) and where the Company recognises those unions. In most cases, information about an individual's trade union membership falls within POPIA's definition of particular personal information (see Part 2 of this Policy for a definition). Therefore, any data relating to employee data subjects' trade union membership will be collected, held, and processed strictly according to the conditions for processing particular personal information, as set out in Part 6.2 of this Policy.

- The Company's lawful basis for processing particular personal information relating to trade unions is in the Labour Relations Act. The following data will be collected and supplied:
    - Name and surname.
    - Employee number.
    - Trade union membership dues.

23. EMPLOYEE MONITORING

The Company may, from time to time, monitor the activities of employee data subjects. Such monitoring may include, but is not limited to, internet, email, and telephonic communication monitoring, vehicle and electronic communication device location tracking, CCTV monitoring of company property, including drivers operating company vehicles, and access control to the workplace and/or for the use of Company equipment. Suppose tracking of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring). In that case, employee data subjects will be informed of the exact nature of the monitoring in advance.

- Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's regular duties.
- Monitoring will only take place if the Company considers it necessary to achieve the benefit it intends to achieve. Personal information collected during such monitoring will only be collected, held, and processed for reasons related to (and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Company's obligations under the Protection of Personal Information Act.
- The Company shall ensure that there is no unnecessary intrusion upon employee data subjects' communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's usual place of work or work hours unless the employee data subject in question is using any Company equipment or other facilities including, but not limited to, Company email, the Company intranet, a virtual private network ("VPN") service provided by the Company for employee use, Company vehicles or electronic communication, storage and computing devices.

24. SHARING PERSONAL INFORMATION OF EMPLOYEE DATA SUBJECTS

The Company will endeavour to share employee personal information only with third parties that have specific safeguards, such as POPIA compliance policies.

- Employee personal information may be shared with clients of the Company, other employees, agents, contractors, or other parties working on behalf of the Company if the recipient has a legitimate, job-related need to know. If any employee's personal information is to be shared with a third party outside of South Africa, the provisions of Part 30 above shall also apply.
- Where a third-party Operator is used, that Operator shall process personal information on behalf of the Company only on the written agreement of the Company and by the guidelines and security measures agreed to.

25. IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of the date of signature by the Director: Corporate Services. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

26. DISCIPLINARY MEASURES

Intentionally or not, contravention of this policy may result in disciplinary action. Such action may include corrective measures, but does not exclude the possibility of termination of employment under certain circumstances.

27. QUERIES

Please contact your HR Representative with any questions or queries about this Policy and Procedure.

28. ANNEXURE: PERSONAL INFORMATION UNDERTAKING

The Employee hereby expressly gives the Employer permission to process any of the Employee's Personal Information, as defined in the Personal Information Legislation:

- For any purposes connected with the Employee's engagement in terms hereof, including but not limited to maintaining personal contact details, complying with applicable legislation, remuneration, implementing health management systems, performance evaluation, training, development planning, occupational health and safety, security and access control, administration, credit references, succession planning, and contingency planning.
- To comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.
- To protect the Employer's legitimate interests in respect of criminal offences which have been, or can reasonably be expected to be, counted against the Employee in the Employer's service.
- For purposes of this clause, "processing" refers to processing as defined in the Personal Information Legislation and includes, but is not limited to, collecting, receiving, recording, organising, collating, storing, updating, retrieving, altering, using, disseminating, distributing, merging, linking, blocking, degrading, erasing or destroying of any Personal Information.

The Employee similarly consents to the lawful processing, analysis, and assessment of the Employee's Personal Information by any other third party, whether based in South Africa or in different jurisdictions. Any Personal Information will only be used by such third parties in accordance with the lawful instructions of the Employer.

- The Employee warrants that any Personal Information provided by the Employee to the Employer shall at all times be true and correct, and that the provision of
- Inaccurate and/or misleading Personal Information shall constitute serious
- Misconduct, subject to appropriate action, including agreement termination.

The processing of Personal Information by the Employer shall further be subject to any applicable lawful policy regulating such processing in place at the Employer, and as amended from time to time in the sole discretion of the Employer.

Signed at _____ on this _____ day of _____ 2025.

Employee

(Name: _____)

For and on behalf of the Employer

(Position: _____)