PROTECTION OF PERSONAL INFORMATION POLICY MANUAL AND COMPLIANCE FRAMEWORK

COMPANY DETAIL

_____ (name and nature of business)

INFORMATION OFFICER DETAILS

_____ has been appointed as Information Officer for purposes of the POPIA. The Information Officer can be contacted at _____ (email address).

INDEX

INTRODUCTION

_____ (name of company) is committed to compliance with, and adheres to, The Protection of Personal Information Act (POPIA) South Africa and confirm that we comply with this legislation. The POPI Act requires us to:

1. Sufficiently inform clients and employees of the purpose for which we will process their personal information.

2. Protect our Information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

We guarantee our commitment to protecting the privacy of our clients, employees, suppliers, and other stakeholders, and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

THE OBJECT OF THE PROTECTION OF PERSONAL INFORMATION POLICY

This Protection of Personal Information Policy seeks to ensure that we:

- comply with legal standards and best practice for the receipt, importing, processing, handling, and storing of personal data of individuals ("Data Subjects"), both as received from its clients, and as held in respect of its own employees;
- protect the rights of our employees, as well as that of our clients and third parties in respect of individuals' data;
- herewith inform how we process individuals' data; and
- protect ourselves from the risks of a data breach.

APPLICATION OF THE PROTECTION OF PERSONAL INFORMATION POLICY

This policy applies to all employees in respect of all personal data accessed in the provision of services by us to our clients, as well as the management of our employment relationships with our own employees.

This policy applies whether personal data relates to a client / supplier / stakeholder or an employee and/or is stored electronically, digitally, on paper, or on other materials, or through other methods.

The appointed Information Officer will ensure compliance with the POPI Act on behalf of the Responsible Party.

RESPONSIBILITIES OF THE RESPONSIBLE PARTY

The Responsible Party must ensure that the principles and conditions relating to processing of personal data described in Chapter 3 of the POPI Act are complied with and be able to demonstrate compliance with them as follows:

- Processing to be lawful, fair, and transparent.
- Data collected is accurate and for specific and legitimate purposes.
- Data collected is limited to only what is necessary.
- Data is kept for time periods no longer than is necessary.
- Data is processed in a secure manner.

- Ensure that the necessary consent is obtained, including parental consent for children.
- Data Subject rights to always be upheld and communications to be as per the provisions of the POPI Act.
- Processing to be performed in accordance with the POPI Act provisions.
- Reasonable records of processing activities to be available.
- Ensure that persons only process personal data as prescribed by the Information Officer.
- Breach and incident notifications to be dealt with as per the organisation's notification policies and procedures.
- Response to breach and incidents to be dealt with as per the organisation's policy and procedures for dealing with these events.
- Data protection Risk and Impact assessments to be done in line with the data risk and impact assessment procedures.
- An Information Officer is to be appointed as per the requirements of the PAIA and POPI Act.
- Cross border or international transfers of personal data information may only be done as per the cross border and international transfer guidelines and only if the Data Subjects' rights are protected in the receiving country.

DEFINITIONS

For the purpose of understanding the terminology used we list the definitions which are referred to in this document.

"consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"Data Subject" means the person to whom personal information relates; in this instance our employees and clients.

"information officer" of or in relation to, a-

(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

(b) private body means the head of a private body as contemplated in section 2, of the Promotion of Access to Information Act.

"personal information" means 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 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;

(*b*) information relating to the education or the medical, financial, criminal or employment history of the person;

(*c*) any identifying number, symbol, email 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 of a 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.

"operator" means a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party.

"processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-

(*a*) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(*b*) dissemination by means of transmission, distribution or making available in any other form; or

(*c*) merging, linking, as well as restriction, degradation, erasure or destruction of information;

"Responsible Party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

POLICY PRINCIPLES AS ENVISAGED IN THE POPIA

1. **Accountability**

It is required that the Responsible Party must ensure that the conditions and all the measures set out in the Act that give effect to such conditions, are complied with at the time of the determining the purpose and means of the processing.

We appointed an Information Officer who will be responsible for overseeing compliance with the provisions of POPI Act. (In the context of a juristic person, information officer means the Chief Executive Officer or equivalent officer of the juristic person.) We have registered with the Regulator the information officer who is responsible for compliance by the company with the provisions of POPIA, working with the Regulator and dealing with requests from Clients and Employees relating to their personal information.

The appointed and registered information officer conducted a personal information impact assessment to ensure that we have adequate measures and protocols in place to comply with the conditions of lawful processing of personal information.

Our Employees must be aware of their accountability with regards to the POPI Act:

- Employees must understand their roles and compliance expectations regarding data protection to keep our organisation compliant with the provisions of the POPI Act.
- Employees must understand the procedures and importance of reporting suspected breaches of security or malware.

- Employees must understand and be prepared for participation in data risk and impact assessments, especially where their department's activities are the subject of the assessment.

2. Processing Limitation

The principle is that personal information may only be processed in a fair and lawful manner and only with the consent of the Data Subject.

Personal information will be obtained directly from the client / supplier or employee unless the information is derived from a public record, or the client and employee has consented to the use of information obtained from another source or has made the information public for instance on social media.

The consent of the Data Subject will be obtained in the event that the personal information has been gathered from a third party if this information is to be shared and used by us. Only information that is required for the specific purpose for which it is gathered will be stored. We may collect more information than required for the intended purpose for future use if we obtain the necessary consent from the Data Subject (this is regarded as "Further Processing" in the Act.)

In line with the principle of minimality, personal information will only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

The Data Subject or competent person may withdraw his, her or its consent at any time. A Data Subject may object, at any time, to the processing of personal information on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

When a Data Subject has objected to the processing of personal information, we may no longer process the personal information.

The personal information in our records should be updated as and when the Data Subject provides new or updated personal information.

2.1 Information we collect directly from the Data Subject

The categories of personal information that we may collect directly from you as client / potential client / supplier / stakeholder include the following: *(Delete which are not applicable)*

- Personal details (e.g. name, age, date of birth, gender, identity number or registration number)
- Contact details (e.g. phone number, email address, postal address or mobile number);
- Customer Details (e.g. VAT numbers, delivery addresses, email addresses, client company details, details of company purchaser)
- Warranty information on product purchases
- Newsletter recipients
- Other stakeholders
- Copies of compliance certification
- Emergency Planning and Operational data
- Environmental plans

- Physical Security plans and contracts
- Transport and Delivery Plans
- Copies of Insurance and Public Liability Insurances
- Client and 3rd party professional qualifications and professional body registration details
- Supplier contracts and supplier contact details
- Customer contracts and customer details
- Details regarding the rendering of services according to instructions given by clients
- Visitor information kept in terms of policies and Covid Regulations.

2.2 Information we may collect from other sources

The categories of personal information for clients / potential clients / suppliers / stakeholders that we may collect from other sources include but are not limited to the Companies and Intellectual Property Commission; Search Works, Financial Institutions; SARS; Google or other search engines.

2.3 Collection of information with regards to employees

The Company collects employee information in a variety of ways. For example, information / data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the Company collects personal information / data about you from social media, third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

The categories of personal information that we may collect directly from the employee or other sources include the following: *(Delete which are not applicable)*

- We require your name, physical address, email address, telephone number, date of birth, gender, identification or passport number as well as the name and contact details of your next of kin/spouse. Without this information we will be unable to employ you;
- We also need to photocopy or scan your ID document / passport / work permit in order to legitimately offer you employment;
- The terms and conditions of your employment;
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- Information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- Details of your bank account;
- Information about your marital status, next of kin, dependants and emergency contacts;
- Information about your nationality and entitlement to work in and outside of South Africa;
- Details of your attendance at work;
- Details of periods of leave taken by you, including holiday, sickness absence and special leave, and the reasons for the leave;
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;

- Assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- We will collect and process additional information about you for career monitoring and advancement opportunities. This may include certain details regarding your racial origin, any disabilities, gender and trade union membership where applicable.

We need your permission to collect the following special information:

- Information about your criminal record;
- Information about medical or health conditions, including whether or not you have a disability or long-term health condition for which the Company needs to make reasonable adjustments;
- Details of trade union membership; and
- Diversity monitoring information, including information about your ethnic origin, sexual orientation, long term health conditions and religion or belief.

3. Purpose Specific

The principle: Personal information may only be processed for specific, explicitly defined and legitimate reasons. Personal information may only be used for the specific purpose for which it was gathered and thereafter it must be destroyed. We will be guided by the applicable legislations pertaining to our various activities to determine when the information held will be destroyed.

At times we are authorised and/or required to collect and/or process personal information in accordance with applicable legislation. A list of the applicable legislation in terms of which records are held by us can be found in our PAIA Manual.

3.1 Client / supplier / stakeholder information

We must have a legal basis to process your personal information. We will only process client / supplier / stakeholder personal information for the purpose(s) for which it was collected and agreed with the client / supplier / stakeholder. In most cases the legal basis will be one of the following:

- to provide services, to the client / supplier / stakeholder, as set out in the agreement or mandate with them or as requested;
- to fulfil our contractual obligations to you for example to ensure that invoices are issued correctly, to communicate with you and to carry out instructions and requests, and to ensure you are able to access our premises when required;
- to comply with our legal obligations to you for example health and safety obligations while we are on any of your premises;
- to comply with our accounting obligations in terms of legislation, such as recordkeeping and tax laws;
- to meet our legitimate interests so that: our products and services comply with your business needs; any complaints or concerns can be promptly relayed and responded to; we may carry out research and analysis to ensure products and services we offer are relevant to you; our records are kept up to date and accurate, and; to send relevant and appropriate electronic correspondence to you in order to keep you informed regarding, but not limited to, industry developments which may impact you, and to invite you to events which are fundamental to the products and services which we provide; and
- contact you with questions regarding the products or services we provide to you.

3.2 Employee information

The processing limitation is especially relevant to the verification of information furnished by applicants for positions when only relevant and adequate information should be sought and verified. Pre-employment records and information will be destroyed when it does not serve any further purpose although the results of the vetting and verification may be retained for longer.

Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA.

Every employee currently employed by us are required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of confidential information.

Each employee that has access to confidential information and works on our IT systems will need to sign a copy of the Electronic Communications and Technology Privacy Policy and the undertaking attached thereto. No Employees and/or Contractors may use the Data Subject's personal information in any way that may be seen as revealing special information deemed to be insulting, disruptive, or offensive by other persons, or harmful to morale.

Where we collect information e.g. pertaining to an employee's health as part of an incapacity enquiry as envisaged in Schedule 8 of the Labour Relations Act 66 of 1995 (LRA) this information cannot be used for any other purpose except that for which it was collected. As such, we cannot process or disclose the information except with the consent of the employee or as required by law.

All information collected about and from potential and existing employees will be handled in compliance with the POPI Act. The personal information as set out but not limited to clause 2.3 of this policy will be used / reflected on / or be processed only as needed and as set out in this Protection of Personal Information Policy. This includes but is not limited to:

- Employment contracts
- Information for completing the Employment Equity Plan
- Disciplinary records
- Salary records
- SETA records
- Disciplinary action taken
- Leave records
- Training records
- Training manuals
- PAYE Records
- Documents issued to employees for income tax purposes
- Records of payments made to SARS on behalf of employees
- All other statutory compliance records, such as Skills Development levies, UIF, COIDA
- General staff administration employee records

3.3 Destruction of personal records

Without consent we may only retain records of personal information for as long as it is necessary to achieve the specific purpose for which the information was collected and as is required by law. We

must however comply with statutory provisions prescribing retention periods such as records for tax compliance and in terms of employment legislation.

In the event that the information is no longer required the destruction of records must be final and, will be done in such a manner, that the records cannot be reconstructed, or the information re-identified. Save for the information that must be retained in terms of applicable legislation, we will undertake the disposal of personal information in line with section 14 of POPIA where e.g. an employment relationship or the relationship with a client / service provider etc. is terminated. There is no stipulated time period set out in POPIA for the destruction and disposal of records of personal information, except that this must happen as soon as reasonably practicable after we are no longer authorised to retain the record.

3.4 Restriction of use of personal information

Processing of personal information will be restricted:

- for a period enabling us to verify the accuracy of the information if its accuracy is contested;
- If we no longer need the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;
- where the processing is unlawful, and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead; or
- where the Data Subject requests to transmit the personal data into another automated processing system.

4. Further Processing Limitation

Personal information may not be processed for a secondary purpose unless that processing is compatible with the original purpose.

4.1 Further processing of personal information

We collect personal information for the reasons set out above. Should we want to use existing personal information for any purpose other than what the information was gathered for, confirmation will be requested from the Data Subject again. The Data Subject will be advised for what the information will be used for and for what period we will hold that information.

The further processing of personal information is not incompatible with the purpose of collection if the Data Subject consented to the further processing or the information is available in or derived from a public record or has deliberately been made public by the Data Subject; if further processing is necessary for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated and the information is used for historical, statistical or research purposes.

4.2 Sharing of information with third parties

In general, we do not share your personal information with third parties (other than service providers acting on our behalf) unless we have a lawful basis for doing so. The Company, for the purposes of carrying out its business and related objectives, does and will from time to time, process Personal Information belonging to a number of persons, including legal entities and individuals.

We rely on third-party service providers to perform a variety of services on our behalf, such as website hosting, third parties who provide IT services, data processing or IT functionality services, for example cloud-based software providers, data analysis providers and data storage or backup providers; electronic message delivery, payment processing, data analysis and research. This may mean that we have to share your personal information with these third parties. When we share your personal information in this way, we put in place appropriate measures to make sure that our service providers keep your personal information secure. These service providers are contractually bound to protect your personal information.

These agreements will be subject to the following conditions:

- Compliance with the provisions of POPIA and the POPIA processing conditions when processing such Personal Information on behalf of the Company;
- Only processing the Personal Information received from the Company in accordance with the mandate or written instruction received from the Company;
- Keeping all the Personal Information held by the Operator on behalf of the Company and / or belonging to the Company Data Subjects, confidential;
- Having measures in place in order to keep all such Personal Information held by the Operator, and processed on behalf of the Company confidential, safe and secure from misuse, abuse and / or unauthorised use or access.

Other situations in which we may disclose your personal information to a third party, are:

- to perform other services, we request from service providers, which may include other firms;
- to fulfil our contractual obligations to you;
- where permitted by law, to protect and defend our rights and property; and
- when required by law, and/or public authorities.

We may also share personal information that cannot identify you for general business analysis, e.g. we may disclose the number of visitors to our websites or services.

4.3 Further processing of personal information of employees

We may, with the consent of an employee, put personal information to further use. In the absence of specific consent from the employee for the further use, we may use the personal information if it is compatible with or in accordance with the purpose for which it was collected in the first place. We must comply with the test for compatibility when for instance passing on personal information to a medical aid or retirement fund, for unemployment benefits or in a business transfer transaction. For example, during the transfer of a business as a going concern in terms of section 197 of the LRA, the old employer is permitted to disclose personal information about its employees to the new employer as required by law.

5. Information Quality

The Responsible Party must take reasonably practicable steps to ensure that the personal information collected is complete, accurate, not misleading and updated where necessary.

By obtaining information directly from the data source, accuracy is more probable. We will always endeavour to validate personal information as it is being captured. If it is not possible for the Data

Subject to input their own information, then the information as captured will be sent to the Data Subject for validation. The Data Subject will be requested to update its personal information by sending a reminder to validate or change the information which will then be captured.

6. Openness

The Data Subject whose information you are collecting must be aware that you are collecting such personal information and for what purpose the information will be used.

We ensure that the Data Subject is aware of the information being collected and the source from which it is collected; the name and address of the Responsible Party; the purpose for which the information is being collected; whether the supply of the information is voluntary or mandatory; the consequences of failure to provide the information; any particular law authorising or requiring the collection of the information; the fact that, where applicable, the Responsible Party intends to transfer the information to a third party; who will receive the information and the right of access to and the right to rectify the information collected and the right to object to the processing of personal information as referred to in section 11(3).

At the time that the personal information is gathered, the Data Subject will be advised of his/her rights to complain to the Information Regulator if misuse is suspected. The Information Regulator's information and contact details will be provided to the Data Subject.

Where personal information is collected from a source other than directly from a Data Subject we are responsible for ensuring that the Data Subject is aware:

- that their information is being collected;
- who is collecting their information by giving them our details;
- of the specific reason that we are collecting their information.

6.1 Employee information

As employer collecting personal information, we must take reasonably practical steps to ensure that the employee is aware of the information collected and the source of the information, the name and address of the Responsible Party, the purpose for which it is collected, whether the employee is obliged to supply the information and what law if any prescribes the disclosure of the information to us.

We will also inform the employee exactly what information will be processed, to whom and the employee's right to access and rectify the information collected or to complain to the Information Regulator. We are obliged to inform the employee before the information is collected from the employee and in any other case either before or as soon as reasonably practicable after collection. When we intend to transfer the information cross border we will inform the employee and also explain to the employee the protection that the information will have in the foreign country or with the international organisation.

7. Security Safeguards

Personal information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorised destruction and disclosure.

Reasonable measures to protect the personal information include identification of possible security risks, establishing and maintaining safeguards against the risks, verifying the safeguards from time to time and updating those measures. Virus programmes, back-ups and off-site storage are all measures to consider. For this purpose we performed a data protection risk impact assessment.

We will ensure technical and organisational measures to secure the integrity of personal information, and guard against the risk of loss, damage or destruction thereof. Personal information is also protected against any unauthorised or unlawful access or processing. We are committed to ensuring that information is only used for legitimate purposes with consent and only by authorised employees of our company. The Information Regulator will be informed in the event of a security breach where personal information could be compromised.

We undertake to:

- put in place strict policies and procedures regarding who has access, and how they gain access, to the personal information in our possession.
- enforce strict policies and procedures to safeguard personal information in our possession. This may include processes to alert us when personal information is accessed or modified without authorisation; to identify the source of a data breach and the procedure to follow to neutralise such a breach.
- have a written contract between us and any operator (service provider), to ensure that the operator establishes and maintains the required security measures. We require from the operator to advise us immediately if there is the possibility that personal data has been accessed or acquired by any unauthorised person.
- mitigate or reduce the risk, in the event of a security breach, through the introduction of control measures; avoid and eliminate the risk through the introduction of controls or introduce new processing methodologies.
- advise you via email or in writing immediately if it is suspected that your personal information has been accessed by unauthorised persons. Sufficient information will be provided to allow you to put measures in place to safeguard yourselves against potential consequences of the security compromise. This may include obtaining your consent to "share" the information or condone the risk.

7.1 Rules for ensuring security safeguards

In order to fulfil our obligations the following rules will be applied:

- All personal data shall be deemed confidential information and be handled as such.
- All security standards will be conveyed to employees that need to access or work on confidential information.
- Employees shall use strong passwords at all times and no passwords will be shared. If passwords need to be shared because of e.g. the absence of an employee, the password will be reset. Only the person/s who need to access data for the execution of their direct work services or required outputs will be entitled to access data.
- Employees should be informed to be vigilant when displaying personal information on computer screens so that unauthorised persons cannot view the data on the screen.
- No data or personal information will be shared outside the scope of required work outputs, or informally. If uncertain an employee shall be entitled to access confidential information only after obtaining authorisation from their line manager or a senior manager, where any work falls outside their normal scope of work.

- Where data is stored on paper, it will always be kept in a secure place where an unauthorised person cannot access or see it. Employees will ensure that paper and printouts are not left in places where unauthorised persons can see them, e.g. on a printer, and all unwanted paper must be shredded.
- Where data is stored electronically, every reasonable attempt will be made to protect from unauthorised access, accidental deletion or any risk of exposure to malicious hacking attempts;
- Where data is stored on removable media such as a CD or a DVD these will at all times be locked away securely when not in immediate use. Data will never be saved directly to laptops or other mobile or removable devices such as tablets or smart phones or sticks or data sticks;
- All data will only be stored on designated drives and servers and will be located in secure protected locations and shall only be uploaded to approved cloud computing services and will be protected by approved security software;
- Regular backups will be made to avoid loss of data or limit it to a minimum;
- Employees will at all times access and update only the central, official copy of any data or work output document, such as payroll.
- Personal data shall never be transferred or sent to any entity not authorised directly to receive it and if sent in the normal cause of business the information will be password protected.

8. Data Subject Participation

Data Subjects may request whether their personal information is held, as well as the correction and/or deletion of any personal information held about them.

Data Subjects have the right to access the personal information we hold about them. They also have the right to ask us to update, correct or delete their personal information on reasonable grounds. Once a Data Subject objects to the processing of their personal information, we may no longer process said personal information. We will take all reasonable steps to confirm our clients' identity before providing details of their personal information or making changes to their personal information.

When you, having provided proof of identity, request information from us on whether we are holding your personal information or the record or a description of the personal information, this request may not be declined and may not be charged for. The full nature and details of the information being held must also be provided on request, but a charge may be levied for this information. You have the right to request the correction of the personal information that we hold and the right to withdraw consent at any time and to be provided with feedback subsequent to the changes or deletion of your information. You are also entitled to know which third parties have or had access to the personal information.

The procedure to obtain the above-mentioned information is covered in our PAIA policies and procedures manual. We may however rely on one of the grounds in the Promotion of Access to Information Act 2 of 2000 (PAIA) to refuse the record or information.

DUTIES OF THE INFORMATION OFFICER

The Information Officer is responsible for compliance with all applicable regulatory requirements regarding the collection and processing of personal information, including but not limited to:

- To collect personal information only by lawful and fair means and to process personal information in a manner compatible with the purpose for which it was collected.
- Where required by regulatory provisions, to inform individuals when personal information is collected about them.
- To treat sensitive personal information that is collected or processed with the highest of care as prescribed by regulation.
- Where required by regulatory provisions or guidelines, to obtain individuals' consent to process their personal information. This includes:
    - Consent from Data Subjects whose information we need for normal business purposes in writing or, in some cases, when responding to enquiries made by users of our website, using rights notices, including the right to withdraw consent at any time, and a consent button on the website.
    - In certain instances, consent is assumed to be automatically given in concluding specific types of contracts. Examples would be Data Subject details when purchasing product or rendering a physical address to which a delivery of product or services is to be made. Documented records will be retained where such processing takes place.
    - Employee data required for tax purposes or by other authorities with a lawful interest is collected by us and processed for these purposes.
    - Where it is in the interest of the Data Subject or as part of a contractual obligation with the Data Subject or in the public interest specific consent will not be sought in such cases.
- To strive to keep personal information accurate, complete and up to date and reliable for their intended use.
- To develop reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, amendment or disclosure of personal information.
- To provide individuals with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or delete personal information.
- To share personal information, such as permitting access, transmission or publication, with third parties only with a reasonable assurance that the recipient has suitable privacy and security protection controls in place regarding personal information.
- To comply with any restriction and/or requirement that applies to the transfer of personal information internationally.

MONITORING

The management and the Information Officer are responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes.

This includes but is not limited to:

- ensuring that all systems services and equipment used for processing and/or storing data adhere to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- issuing appropriate, clear, regular rules and directives, whether for the organisation as a whole or a particular part of it, department, person or level of person in relation to any aspect of the company's work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.
- evaluating any third-party services the company is considering or may acquire to process or store data, e.g. cloud computing services.

RIGHTS OF DATA SUBJECTS IN SUMMARY

Please let us know if any of the personal information that we hold about you changes so that we can correct and update the personal information on our systems. The following are the rights that you may exercise:

1. **Right of access to information**

You have the right to request, free of charge, confirmation as to whether we hold personal information about you. You also have the right to request a copy of the record of personal information or a description of the personal information we hold about you. Submission of access request forms together with the details of the access request procedure can be found in our PAIA Manual. For more information contact our Information Officer.

2. Right to request correction or deletion of personal information

You can request, where allowed by law, the correction, updating or deletion of the personal information held by us. You can also request, where allowed by law, the destruction or deletion of a record of information held by us. Submission of a request for correction or deletion forms together with the details of the request for correction and deletion procedure can be found in our PAIA Manual. For more information contact our Information Officer.

3. Right to object to the processing of personal information

In certain circumstances, such as when we process your information for our or your legitimate interests, you may object to the processing of your personal information, unless we are required to process the information on another basis, such as a legal basis. Submission of objection forms together with the details of the objection procedure can be found in our PAIA Manual. For more information contact our Information Officer.

4. Right to ask us to share your personal information in a usable format with another entity

We can provide the personal information which you provided to us, to you or another person, in commonly used and machine-readable format.

5. Right to object to automated decision-making and profiling

Where we use automated decision-making or profiling to make decisions, you may object to this profiling. Alternatively, you may ask that a person review a decision made, or that you be provided with the logic around such a decision, so that you can make a representation in respect of the decision.

6. Right to unsubscribe from direct marketing

Where you do not wish to receive marketing communication from us, you can unsubscribe from marketing emails by clicking on the unsubscribe link in each email.

We will still be able to contact you when there is important communication required to be sent.

7. Right to withdraw consent

Where you have given your consent to a particular type of processing, you may withdraw that consent at any time by contacting us using the contact details set out below.

8. Right to lodge a complaint with the Information Regulator

You have the right to lodge a complaint with the Information Regulator, in the prescribed manner and form, if you believe that we are interfering with the protection of your personal information. You can contact the Information Regulator on 010 023 5207 (telephone number) and can lodge a complaint via email on inforeg@justice.gov.za.