RAISE GLOBAL SA (PTY) LTD

2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

DATA PRIVACY POLICY

AUGUST 2023

Table of Contents

1. Why we have this policy

We have this policy to help guide our actions so that we keep our customers, employees and suppliers/service providers data safe, protect our reputation, and comply with all relevant data protection regulations, including the Protection of Personal Information Act (POPIA).

2. The Scope of this policy

This policy applies to:

- Any activity where we produce or use personal information (processing activities);
- Anybody involved in processing activities where we produce or use personal information;
- All employees, service providers, contractors, and other individuals who have access to personal information.

3. Why is it important to comply with this policy

3.1 If the organisation does not comply

Our reputation is our biggest asset. Without our reputation, our relationships with key stakeholders and investors would suffer. In addition, we could face substantial fines.

3.2 If you do not comply

This organisation only works when we all do our part, and all of us want to see the organisation succeed. If you do not comply with this policy, or if you discover that we are not complying with the policy and you do not tell us about it, you could face disciplinary action.

4. Our Policy

While all personal information should be protected, we take a risk-based approach to compliance. We prioritise the protection of personal information that is used in our important business activities, and in activities that could have a substantial impact on a data subject's right to privacy.

It is our policy to:

- follow the principles of privacy protection that are set out in the POPIA; and
- conduct data protection impact assessments.

4.1 We follow the principle of data privacy

THE PRINCIPLE	WHAT WE DO
Classify personal information	We identify and classify the personal information that we use and produce.

Document processing activities	We document all processing activities to ensure that we can respond to requests from the Information Regulator and requests for information by data subjects or third parties.
Specify the purpose for processing	We specify and document the purposes for which we process personal information.
Provide legal basis for processing activities	We ensure that: ● All processing activities have a legal basis; and ● We document the specific legal basis for processing personal information for each activity.
Keep processing to a minimum	We ensure that: ● we process personal information that is adequate, relevant, and not excessive, considering the purpose of the activity; and ● we de-identify personal information before we start the activity where possible. Where de-identification is not possible, we must consider masking the personal information.
Obtain personal information from lawful sources	We obtain personal information from lawful sources only. Lawful sources of personal information include: ● The data subject; ● information that the data subject made public deliberately; ● public records; and ● a source that the data subject consented to. Other sources may be lawful in special circumstances. If you are unsure, speak to the Deputy Information Officer.
Process transparently	We disclose all processing activities to data subjects in our privacy notices.
Ensure personal information quality	We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.
Limit sharing	We only share personal information if it is legal to do so and ethically justifiable. We: ● identify all instances when personal

	information is shared with external organisations or individuals (third parties); ● ensure that sharing personal information complies with data protection legislation and the Information Sharing Procedure; ● enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information; ● conduct an information sharing assessment to determine who is responsible to ensure that contracts are concluded, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing; ● keep record of personal information sharing activities, including the outcome of assessments, a record of additional steps taken, what personal information was shared and when, and the method we used to share the personal information.
Keep personal information secure	We protect all personal information that we use and produce against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information. All personal information processing must comply with our Information Security Management Policy.
Manage personal information incidents	All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure. An incident includes: ● non-compliance with this policy and any procedures that relate to it; ● contraventions of any data protection legislation such as the POPIA; and ● security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information. Employees must immediately report: ● any known or suspected incidents; or ● any circumstances that increase the risk of an incident occurring. Reports must be sent to dany.mawas@raisefx.com
Manage retention periods	We ensure that all records: ● are managed appropriately and in accordance with any operational or

	legal rules that may apply; and ● comply with our Records Management Policy.
Respect data subjects' rights	We respect the rights of data subjects to: ● access their records; ● know who their information was shared with; ● correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information; ● withdraw consent; and ● object to the processing of their information when it is not necessary for the conclusion or performance of a contract or to comply with an obligation imposed by law. All data subject requests must go through the Data Subject Request Procedure.

4.2 We conduct personal information impact assessment

Senior Management must ensure that a personal information impact assessment is done before we start a new processing activity. The data protection impact assessment must include a risk analysis of the activity.

We must conduct a personal information impact assessment before we:

- continue to process personal information as part of an activity that has not undergone a data protection impact assessment before;
- change an existing processing activity;
- launch a new product or service;
- expand into other countries;
- use new systems or software for processing personal information; or
- share personal information with third parties.

A personal information impact assessment has three phases:

- Identify activities in which personal information is processed.
- Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.
- Complete a further investigation and assessment with assistance from the Deputy Information Officer if the activity had a risk rating of high or critical after the data protection impact assessment questionnaire was completed.

All activities that are rated as critical or high risk during the data protection impact assessment must undergo an assessment every three years.

5. Roles and Responsibility

These are the responsibilities in respect of this policy:

The Information Officer (*Dany Mawas)*	Our Regional Director for Africa is our Information Officer. The Information Officer has a coordinating function that focuses on the policy-based protection of our information and is the policy owner of this policy. The Information Officer must ensure that this policy receives support from senior management throughout the organisation and that senior management discharges their responsibilities.
Deputy Information Officer (*Charmaine Mavhunga)*	Deputy Information Officers must support the Information Officer and are responsible for strategic guidance to the organisation on data privacy risk management. The Deputy Information Officers must: ● oversee the implementation of this policy, ● develop procedures and standards to support data privacy, ● provide advice on the identification and management of data privacy risk, ● monitor whether personal information impact assessments are performed when required, ● develop training on data privacy, ● respond to data subject requests and objections, ● respond to requests from the information regulators and working with regulators when there is an investigation, ● monitor whether this policy is implemented throughout the organisation.
Director of IT	The Director of IT supports the Information Officer and the Deputy Information Officers by: ● developing Information Technology policies, procedures, standards and guidelines; ● providing technical advice on data privacy; ● supporting the implementation of this policy through appropriate technology investments; ● ensuring that the organisation only invests in information technology that complies with this policy.
Senior Management	Senior Management must implement this policy, create or align other policies and processes in their business areas with this policy, and monitor and advocate for compliance within their business areas. Senior Management must ensure that:

	● business areas comply with this policy; ● a register of information assets used in important information processing activities in their business area is created and maintained; ● information used in important information processing activities is classified; ● personal information impact assessments are conducted before confidential and personal information is processed; ● data privacy-related risks in their business area are managed; and ● their business area participates in investigations into incidents.
Users of information	All users who have access to the organisation's information or information systems must: ● adhere to all policies, procedures and guidelines that relate to the use of information; and ● report any actual or suspected incidents.
Internal and external audit	Internal and external audit provides independent assurance that the organisation's risk management, governance and internal control processes are operating effectively, including compliance with this policy.

6. Our policy glossary

Data subjects	The person or organisation to whom personal information relates. This includes: ● prospective customers ● customers; ● staff members and job applicants; ● service providers, contractors, and suppliers; ● shareholders and directors; and ● members of the public and visitors.
Incident	An incident includes: ● non-compliance with this policy and any procedures relatin to it; ● contraventions of any data protection legislation such as the POPIA; and ● security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.

Processing activities	Processing activities are a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored, or destroyed. A processing activity is important if we could experience critical or high levels of risk if the process or activity is disrupted or could no longer continue.
Personal information	Personal information means any information relating to an identifiable individual (living or deceased) or an existing organisation (a company, public body, etc.). This includes the personal information of all customers, staff members, job applicants, shareholders, board members, service providers, contractors, suppliers, members of the public, and visitors. Examples include: ● identifiers, such as a name, identity number, staff number, account number, customer number, company registration number, tax number, photos, videos, or any other unique information that can be used to identify a person; ● demographic information, such as race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, religion, conscience, belief, culture, language, and birth; ● information relating to physical or mental health, wellbeing, or disability; ● background information, such as education, financial, employment, medical, criminal or credit history; ● contact details, such as physical and postal address, email address, telephone number, online identifier (e.g. a person's twitter handle) or location information; ● biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioral characterisation, such as blood-typing, fingerprinting, DNA analysis, retinal scanning, facial recognition, and voice recognition; ● someone's opinions, views, and preferences; ● private or confidential correspondence and any further correspondence that would reveal the contents of the original correspondence; ● views or opinions about a person, such as interview notes and trade references; and

	• the criminal behavior of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject.
POPIA	The Protection of Personal Information Act 4 of 2013 and its regulations
POPIA Programme	The POPIA Programme is our ongoing efforts to comply with the provisions of the POPIA and includes: • stakeholder consultation; • defining roles and responsibilities; • policy development; • policy implementation; • monitoring and audit; and • continual improvement.
Processing	Any operation or activity or any set of operations concerning personal information, including: • collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using; • disseminating by means of transmission, distributing, or making available in any other form; or • merging, linking, restricting, degrading, erasing, or destroying personal information.

7. Supporting Documents

You must read this policy with:

- Data Subject Request Procedure
- Personal Information Impact Assessment Procedure and assessment

VERSION HISTORY

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**Dany Mawas**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**

RAISE GLOBAL SA (PTY) LTD
2018/616118/07

An authorised Financial Services Provider* with *FSP No: 50506

POPIA MANUAL

August 2023

Contents

Definitions

"biometrics" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

"code of conduct" means a code of conduct issued in terms of Chapter 7

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

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"data subject" means the person to whom personal information relates;

"de-identify", in relation to personal information of a data subject, means to delete any information that—

(*a*) identifies the data subject;

(*b*) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(*c*) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"de-identified"** has a corresponding meaning;

"electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"filing system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"information matching programme" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

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

(*b*) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"person" means a natural person or a juristic person;

"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, 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 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;

"private body" means—

(*a*) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(*b*) a partnership which carries or has carried on any trade, business or profession; or

(*c*) any former or existing juristic person, but excludes a public body;

"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;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

"public record" means 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;

"record" means any recorded information—

(*a*) regardless of form or medium, including any of the following—

(i) Writing on any material;

(ii) 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;

(iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) 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;

(*b*) in the possession or under the control of a responsible party;

(*c*) whether or not it was created by a responsible party; and

(*d*) regardless of when it came into existence;

"Regulator" means the Information Regulator established in terms of section 39;

"re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

(*a*) identifies the data subject;

(*b*) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(*c*) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

"Republic" means the Republic of South Africa;

"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;

"restriction" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"special personal information" means personal information as referred to in section 26;

"this Act" includes any regulation or code of conduct made under this Act; and

"unique identifier" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

Introduction

Raise Global SA (Pty) Ltd is an authorised Financial Services Provider and thus governed by the Financial Advisory and Intermediary Services Act (The "FSP" hereafter) and a Private Company registered in the Republic of South Africa under registration number 2018/616118/07. Raise Global SA (Pty) Ltd as a corporate and ethical citizen subscribes to the protection of personal information. The institution has therefore set up a manual to assist the governing body, management, and employees of Raise Global SA, to accomplish the requirements set by Parliament to address the ramifications associated with the probable misuse of information collected by Raise Global SA pursuant to its business relationships and interactions. Raise Global SA as a responsible party respects the right to promote and protect the rights enunciated in the various Bills, Acts and regulations stated below, but is also cognisant of the fact that such right must not infringe the right to economic and social progress through the removal of barriers to the free flow of information including personal information. Hence, Raise Global SA as an

organisation and in its processes, will endeavour to bring a balance between those personal and economic rights for the benefit of the economy, its institution, and its stakeholders.

It is critical for the organisation to comply with this manual to avoid reputational damage, maintain good client relationships and to avoid fines and litigation.

Background

Prior to the introduction of Personal Information Act, no 4 of 2013, the public was exposed to unregulated processes of collecting, retaining, and sharing personal information with third parties. The Parliament pursuant to the right to privacy and to manage the mischief related to the misuse of personal information, sort to introduce legislation and regulations to protect the right to privacy enshrined in the Constitution and to regulate the use of information. The legislation seeks to regulate information processed by private and public bodies; to set minimum requirements for processed information and to set standards for sharing information across borders.

The law and regulations will in essence protect information and privacy, prevent harm to the public, manage the theft of personal identities and minimise fraud against persons, entities or legal bodies and the country. The information may relate to individuals, juristic persons, partnerships, trusts, or other. The Regulator has introduced various mechanisms to safeguard personal information including the appointment of suitably qualified persons in senior positions to act as information officers charged with the responsibility.

Governing body resolutions relating to compliance

Raise Global SA (Pty) Ltd governing body endorses the Protection of Personal Information Manual introduced pursuant to the Protection of Personal information Act no. 4 of 2013. Raise Global SA seeks to align its business objectives and purpose to the spirit and letter of the law through the implementation of the POPI manual. The code of ethics values personal information collected by Raise Global SA and endeavours to protect and share same in accordance with the laws and regulations. In the quest to safeguard personal information Raise Global SA has appointed suitably qualified personnel to manage the process and ensure that compliance is maintained continuously and that all processes are indicative of the spirit and letter of the law. In addition, the responsibility to manage the risk associated with personal information is and remains the responsibility of every employee of Raise Global SA regardless of rank or position.

Executive management commitment

The Executive management of Raise Global SA has the delegated responsibility of the governing body to embrace, embed and manage appropriate processes to process information and is accountable to the board for its actions or omissions. Executive management must ensure that where necessary they engage or appoint the necessary expert knowledge or advice to manage the processes. Executive

management's commitment to the process must be seen and enunciated throughout the organisation both in its deeds and attitude.

Compliance function

The Information Officer (IO) with the assistance of management is responsible for compliance with the Protection of Personal Information (POPI) POPI manual. The IO is Mr Dany Mawas and is registered with Information Regulator. The IO with the approval of management and the board will set up systems to implement and manage the process documented in the manual. The IO has a mandate to ensure that the manual is continuously updated and remains relevant. The manual may be reviewed quarterly, annually or as the need arises. All stakeholders may contact the IO for any queries or redress by following the appropriate process. The IO may be contacted via email and telephonically on the following details:

Email: dany.mawas@raisefx.com

Telephone: 082 042 2064

Compliance Stakeholders

Raise Global SA stakeholders include the board, management, employees, its limited partners, related contractors, suppliers and other third parties as may be required to support the activities of Raise Global SA in the implementation of various projects. Raise Global SA has a duty to respect the rights of all stakeholders as far as it relates to personal information or rights enunciated in the Protection of Personal Information Act 4 of 2013 (POPI Act), it's applicable codes of conduct as may be amended from time to time and the Raise Global SA manual. Where necessary Raise Global SA may engage stakeholders to ascertain their satisfaction or dissatisfaction with internal processes or to garner intuitive ways to processes and safeguard information.

Compliance Obligations

Raise Global SA has an obligation in terms of the POPI Act to:

> Collect data **directly** from the source **unless** the data has been made public, collection from another source will not directly infringe the right of the data subject; if it necessary to conduct proceeding in a court of law; to avoid prejudice to the maintenance of a law by a public body; for national security; for the legitimate interest of the responsible party or third party; if compliance would prejudice a lawful collection or if compliance is not be reasonably practicable in the prevailing circumstance.
>
> use the Personal Information collected for a lawful, explicitly defined purpose, relating to the activity of the responsible party in terms of Section 9 of POPIA and shall not be in excess for the purpose for which it is required.

ensure that the collection and processing of information of the Data Subject will not prejudice the Data Subject in any form or manner and should this situation occur, the information will be immediately erased.

Ensure that the Data Subject hereby confirms that the consent to process Personal Information is voluntary, specific, and informed and may be withdrawn at any time during the relationship subject to specific conditions being met.

Ensure that the Data Subject acknowledges that consent does not apply to the processing of information relating to sections 26 to 33 of POPIA: the exceptions for special personal information relating to the below:

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 alleged criminal offence or proceedings

ensure that the Data Subject appreciates that in terms of section 27 of POPIA, the exception is subject to limitations and does not apply if the processing is carried out with the Data Subject's consent or in fulfilment of a right or obligation in law, for international public law purposes, for historical or statistical reasons or the information has been made public.

Ensure that the Data Subject understands and accepts the processes that govern the consent, justification and objection to the collection and processing of the Data Subject's Personal Information under POPIA.

Ensure that the data subject is aware of their right under the Promotion of Access to Information Act 2000, to access their personal information and request the deletion or destruction of personal information where applicable.

Compliance Process

Raise Global SA has an obligation to ensure that all the areas provided for in the POPI Act are addressed and appropriate processes adopted to manage those areas. Raise Global SA processes are articulated below. The Responsible party with the assistance of the IO is responsible for setting up systems that promote the legal processing of personal information.

1. **The responsible party must identify mechanisms or systems that process personal data within the organization**

These may be electronic processes such as IT systems, cloud computing, websites, applications, any new systems, or systems under development or otherwise. Raise Global SA must ensure that these processes comply with the privacy requirements. Systems that process information must be documented in the Raise Global SA repository. Access controls assigned to the system must remain active throughout the life of the system.

2. **The responsible party must ensure that it has obtained consent from the data subject to process information except for situations that are exempted.**

Consent from the data subject is a requisite to the processing of personal or sensitive personal information. The validity of consent is subject to meeting all the legal requirements. Raise Global SA processes data relating to staff for legitimate reasons, this often does not require consent, however where consent is required in fulfilment of a laws or regulations, this is obtained from the data subject.

3. **The responsible party must ensure that the information obtained from data subjects is for legitimate business purposes.**

Information obtained from the subject data must be for legitimate business purposes, hence it must not exceed that which it is purposed to accomplish. Raise Global SA should consider whether the legitimate business considers all possible data processing requirements including possible breaches. Information obtained for legitimate business will vary according to the type of data subject, for example, employee, contractors, suppliers, limited partners etc. Should Raise Global SA require information for statistical purposes other, this would be a secondary requirement to the legitimate purpose and must be aligned to such purpose.

4. **The responsible party must ensure that the information obtained from employees is for legitimate business purposes.**

Information obtained from employees must be for legitimate business purposes. In this case it would be aligned to human resources and personnel management as it relates to the employment contract. Hence typically information to be obtained would be birth date, identification number, previous employment history, qualifications, gender, disability (for purposes of employment equity and needs analysis), contact details of family members or friend for emergency purposes, information relating to immediate family to assess requirements for compassionate leave, family responsibility and work/balance initiatives.

The information will be regulated based on the purpose for which it is required, for example, for the performance or termination of an employment contract, recruitment, compensation and benefits, pension, social security information, travel and expenses, performance evaluations, for employee communication, for management of the business such as managing finances, scheduling work and responsibilities, implementing controls, health safety and security of employees, for the purpose of conducting investigations, defending claims or litigation for legal or regulatory compliance. The list is not exhaustive and other instances that require employee information may arise and will be addressed within the legal confines.

5. **The responsible party must ensure that the information obtained from its business associates is for legitimate business purposes.**

Information obtained from business associates will vary depending on the nature of the business, the risk exposure posed by the relationship and the duration of the relationship. Information may relate to relationship management, the development and execution of strategies, asset management, de-mergers, and mergers, to facilitate acquisitions and divestitures, to inform internal audits and investigations, for the implementation of controls or for management reporting. The information requested may be financials, management accounts, company registration documents, directors and shareholder information, contracts secured or legitimately expected, conflicts of interest register, among other things.

6. **The responsible party must ensure that the information obtained from suppliers or contractors is for legitimate business purposes.**

Sensitive information relating to the personal data of suppliers or contractors may only be processed for specific reasons within the confines of applicable laws and regulations. In cases where the request for sensitive information is not within the list of legitimate requirements but is required by a specific claw or regulation prior approval must be obtained from the IO and legal to ensure that the purpose is aligned and to manage any breaches or litigation.

7. **The responsible party ensure that the information obtained is relevant and accurate for the purpose for which it is required**

Information obtained must be relevant for the purpose for which it is required. The IO with the assistance of staff must ascertain that the information is accurate by either using public sources to verify the veracity of the information or other as may be assigned by the organization. Failure to verify the accuracy of information may pose a risk to the organization both financially and reputational. Inaccurate or redundant personal data must be erased without delay to comply with the relevance and accuracy requirements. Request from data subject to update personal information must be attended to without delay and must not be in excess for the business purpose. Records must be retained and disposed of in line with applicable laws, for guidance, properly disposed within five years of terminating a business relationship. The disposal processes used by the organization must be followed.

8. **The responsible party ensure that the information obtained must be used for the purpose for which it is was collected.**

Raise Global SA has a duty to implement mechanisms to regulate access to personal data by staff and to ensure that stuff with access to information only use it for the intended purpose. Data subjects must be adequately informed regarding the processing of their data. The explanation must be simple, clear, transparent, and concise to avoid any ambiguity. Transparency regarding the intended use of the personal data is critical to the protection of personal information. Raise Global SA must be able to assess the impact of processing personal information, the degree of necessity and whether information

gathered is proportionate to the intended use. Processes and controls must be implemented to manage risks associated with excessive collection and use of personal data.

9. The responsible party must ensure that information is secure and safe from any breaches

The organisation must implement processes to protect the information collected from misuse, unauthorised access, or disclosure whether accidental or other, loss or destruction, inaccessibility, or unlawful acquisition by another. The use of passwords, encryption, access codes. Raise Global SA is responsible for the safe keeping of personal information, including that which may be processed by third parties engaged by Raise Global SA, for instance health insurers, pensions funds, vehicle hire companies. Information shared with third parties must be adequate for the intended purpose and Raise Global SA remains responsible for any breach in the processes of sharing or gathering information. Raise Global SA is not responsible for breaches that arise through sharing information with a third party such as a government body or required in fulfilment of a legal obligation. Where information is shared international appropriate contractual clauses that safeguard personal information must be included in the agreements.

10. The responsible party must ensure that there are appropriate processes to report any breaches

Staff must report any breaches to personal information immediately and timeously to manage associated risks such as reputational damage and to manage business relationships. Staff must report the breaches internally and not to a third party. A breach may relate to the unlawful processing of personal information or to the code of conduct issued by the Information Regulator. The Information Regulator may from time to time provide a code of conduct to manage the processing of information. Any breaches to the Raise Global SA internal processes of personal of information are subject to the code of conduct and are a direct breach of the code in operation at the time.

All relevant authorities must be informed immediately of any breaches whether actual or suspected. Breaches may be committed by Raise Global SA or its third parties. Breaches to personal information may trigger certain rights of data subjects. Data subjects have individual rights to control the use of their personal data, access their data, request for deletion, or withdraw consent to use the data. Raise Global SA must respect such decisions and facilitate the process of access, limitation, or withdrawal within the prescribed legislated timelines. Staff must be made aware of the rights of data subjects, to adequately assist with the process.

11. The responsible party ensure that there is a complaints process to report any breaches to information.

Raise Global SA has a complaints process for data subjects. The process is aligned with legislative requirements. Data subjects have a right to lodge a complaint where they feel their rights to confidentiality has been breached. The breach may occur during the process of obtaining, storing, processing, or sharing their personal information. Raise Global SA takes all complaints very seriously

and complaints will be addressed timeously through the appropriate channels within the legislated timelines.

Internal complaints process

The IO has the ultimate authority to decide whether there has been a breach and the appropriate remedy to resolve the breach. Raise Global SA may also restrict the use of personal information while they consider the legitimacy of the rights exercised by the data subject. A responsible party or data subject who is dissatisfied with the outcome of a compliant may approach the adjudicator of Information Regulator for redress.

External complaints process

Any person may report a compliant to the Information regulator in writing. The Information regulator has a duty to provide reasonable assistance to the complaint to enable one to formulate a written complaint should the assistance be required. The Responsible party or data subject also has a right to lodge a complaint with the Information Regulator should they be aggrieved with the outcome of the decision of the adjudicator. Upon receipt of a complaint the IR may decide to investigate the complaint, refer the complaint for enforcement or may decide not to act upon the complaint.

Training and awareness

The Information Officer of Raise Global SA is tasked with making sure that all employees of the organisation receive appropriate training regarding the processing of information to manage the risk exposure within their working environment. Raise Global SA staff have a duty to understand what personal information is processed by the organisation and the procedure. The organisation must involve the staff in the assessment of personal information to ensure that they understand the importance of the Act. There shall be no excuse or ignorance, attributed to the lack of access to information from any employee. Failure to comply with this manual or to inform the organisation of any non-compliance that one is aware of could result in disciplinary action. The manual will be made available to all personnel to ensure that all possible risks are managed and that all employees are suitably informed and equipped. Any changes to processes shall be communicated to all personnel through the issuance of an updated manual.

Relationship with regulators/supervisors

The Information Officer has the authority to liaise with the regulator regarding any information to be communicated to the regulator or in relation to any information requested by the regulator. Raise Global SA position is to maintain a cordial and respectful relationship with the regulator.

CONSENT TO THE COLLECTION AND PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11 OF THE PROTECTION OF PERSONAL INFORMATION ACT NO.4 OF 2013

I, ……., *)* a director of Raise Global SA (Pty) Ltd do hereby give consent for Raise Global SA (Pty) Ltd (, to collect and process my Personal Information in terms of section 11 of the Protection of Personal Information Act No. 4 of 2013 (***hereinafter referred to as*** **"POPIA").**

The responsible party hereby undertakes to use the Personal Information collected for a lawful, explicitly defined purpose, relating to the activity of the responsible party in terms of Section 9 of POPIA and shall not be in excess for the purpose for which it is required.

The responsible party undertakes to ensure that the collection and processing of information of the Data Subject will not prejudice the Data Subject in any form or manner and should this situation occur, the information will be immediately erased.

The Data Subject hereby confirms that the consent to process Personal Information is voluntary, specific, and informed and may be withdrawn at any time during the relationship subject to specific conditions being met.

The Data Subject acknowledges that consent does not apply to the processing of information relating to sections 26 to 33 of POPIA: the exceptions for special personal information relating to the below:

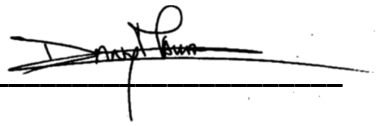
> religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
> alleged criminal offence or proceedings

The Data Subject appreciates that in terms of section 27 of POPIA, the exception is subject to limitations and does not apply if the processing is carried out with the Data Subject's consent, in fulfilment of a right or obligation in law, for international public law purposes, for historical or statistical reasons or the information has been made public.

The Data Subject understands and accepts the processes that govern the consent, justification and objection to the collection and processing of the Data Subject's Personal Information under POPIA.

This POPIA Manual has been adopted as follows:

Signed this 28th day of August 2023

Signature 

Dany Mawas

Forms that applicable to the processing of personal information as provided for by the Information Regulator:

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11 (3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2.]

Note:

1.Affidavits or other documentary evidence as applicable in support of the objection may be attached.

2.If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3. Complete as is applicable.

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	

	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	REASONS FOR OBJECTION IN TERMS OF SECTION 11 (1) (*d*) to (*f*) (Please provide detailed reasons for the objection)

Signed at_____this day Of _____ /2022.

_____
Signature of data subject/designated person

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24 (1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013
(ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3.]

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.

2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3. Complete as is applicable.

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	

Fax number/E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	INFORMATION TO BE CORRECTED / DELETED / DESTRUCTED / DESTROYED
D	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (*a*) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (*b*) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN (Please provide detailed reasons for the request)

Signed at this day of 20	
	.....
	Signature of data subject/designated person

RAISE GLOBAL SA (PTY) LTD
2018/616118/07

PROTECTION OF PERSONAL INFORMATION (POPI) POLICY

An authorised Financial Services Provider FSP No: 50506

September 2023

1. Protection of Personal Information Policy

Objective:

The objective of this policy is to protect Raise Global SA (PTY) LTD information assets from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy establishes a general standard on the appropriate protection of personal information within Raise Global SA (PTY) LTD It provides principles regarding the right of individuals to privacy and to reasonable safeguards of their personal information.

Scope:

This policy applies to the sole proprietor or key individuals, representatives and staff of Raise Global SA (PTY) LTD. The company and key individuals (or management) are ultimately responsible for ensuring that information security is properly managed. The Information Officer, Dany Mawas is responsible for:

- The development and upkeep of this policy.
- Ensuring this policy is supported by appropriate documentation, such as procedural instructions.
- Ensuring that documentation is relevant and kept up to date.
- Ensuring this policy and subsequent updates are communicated to relevant managers, representatives, staff and associates, where applicable.

The company and all key individuals, representatives and staff are responsible for adhering to this policy, and for reporting any security breaches or incidents to the Information Officer.

The external individual(s) who is (are) contracted to handle the information technology of Raise Global SA (PTY) LTD must adhere to the same information security as that of Raise Global SA (PTY) LTD and will confirm by separate agreement that they have such security measures in place in respect of processing of personal information.

Key Principles:

The company and each key individual, representative and staff member of Raise Global SA (PTY) LTD is committed to the following principles:

- To be transparent with regards to the standard operating procedures governing the collection and processing of personal information.
- To comply with all applicable regulatory requirements regarding the collection and processing of personal information.
- 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.
- 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, unauthorized 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 Information Officer of Raise Global SA (PTY) LTD 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. The company and key individuals, representatives and staff of Raise Global SA (PTY) LTD are to be trained according to their functions in regulatory requirements, policies and guidelines that govern the protection of personal information. Raise Global SA (PTY) LTD will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with privacy regulation, policy and guidelines.

Operating controls:

Raise Global SA (PTY) LTD shall establish appropriate privacy standard operating controls that are consistent with this policy and regulatory requirements. This will include:

- Allocation of information security responsibilities.
- Incident reporting and management.
- User ID addition or removal.
- Information security training and education.
- Data backup.

Implementation:

This policy is implemented by Raise Global SA (PTY) LTD and will be adhered to by the company and all key individuals, representatives and staff who are tasked with collecting and processing of personal information. Non-compliance with this policy may result in disciplinary action and possible termination of employment or mandate, where applicable.

Signed this 1st Day of September 2023.

David Bottin

Director

RAISE GLOBAL SA (PTY) LTD
2018/616118/07

An authorised Financial Services Provider with FSP No: 50506

THE PROMOTION OF ACCESS TO INFORMATION ACT

August 2023

Table of Contents

1. Introduction

Raise Global SA (Pty) Ltd a company registered in South Africa with registration number 2018/616118/07 and with registered address Oxford Glenhove Building 2, 114 Oxford road, Rosebank, Gauteng, 2196, South Africa, it is authorized and regulated by the South African Financial Sector Conduct Authority (FSP 50506) .

The Corporate Governance Policy sets out the framework on which the FSP's corporate governance structures and processes are based. The Corporate Governance Policy sets out the decision-making structures of the FSP and how the decision-making structures support and assess one another to achieve the King IV objectives of ethical leadership and effective leadership. It is also to facilitate the governance of the organisation in a fair, transparent, responsible, accountable, and ethical manner by the board, management and all personnel. The framework will imbed the principles of Treating Customers Fairly (TCF) that run through the recently promulgated Fit and Proper requirements.

2. Company Contact Details

Director / Information Officer: Dany Mawas

Postal Address:	Oxford & Glenhove Building 2, 1st Floor, 114 Oxford Road, Rosebank, Johannesburg, 2196
Street Address:	Oxford & Glenhove Building 2, 1st Floor, 114 Oxford Road, Rosebank, Johannesburg, 2196
Telephone Number:	+27 82 042 2064
Fax Number:	None
Email:	dany.mawas@raisefx.com

3. The Act

3.1 The Act grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

3.2 Requests in terms of the Act shall be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are provided herein as stipulated by the Act.

Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission, which will contain information for the purposes of exercising Constitutional Rights.

The guide can be obtained upon request during normal working hours from:

- the Information officer of "Raise Global SA" including the office of the regulator.Details of the information officers are provided below:

  Information Officer – Dany Mawas – dany.mawas@raisefx.com

  Deputy Information Officer- Kevin Wides – kevin.wides@raisefx.com

- the website of the Regulator (https://www.justice.gov.za/inforeg/)

3.3 The contact details of the Commission are:

Postal Address:	Private Bag 2700, Houghton, 2041
Telephone Number:	+27-11-877 3600
Fax Number:	+27-11-403 0625
Website:	www.sahrc.org.za

4. Application Legislation

No	Ref	Act
1	No 61 of 1973	Companies Act
2	No 98 of 1978	Copyright Act
3	No 55 of 1998	Employment Equity Act
4	No 95 of 1967	Income Tax Act
5	No 66 of 1995	Labour Relations Act
6	No 89 of 1991	Value Added Tax Act

7	No 37 of 2002	Financial Advisory and Intermediary Services Act
8	No 75 of 1997	Basic Conditions of Employment Act
10	No 25 of 2002	Electronic Communications and Transactions Act
11	No 2 of 2000	Promotion of Access of Information Act
12	No 30 of 1996	Unemployment Insurance Act

5. Schedule of Records

Records	**Subject**	**Availability**
Administration	• License information	Freely available on web site www.raisefx.com/
Human Resources	• Employment Contracts • Remuneration Records and Policies • Records of Disciplinary Hearings • Staff Salaries and Benefits	From Information Officer upon request
Client Registry	• Particulars of client	From Information Officer upon request
Public Affairs	• Public Product Information • Public Corporate Records • Media Releases	Freely available on web site www.raisefx.com/
Financial	• Financial Statements • Financial and Tax Records (Company &Employees) • Asset Register • Management Accounts	Proprietary - Request in terms of PAIA.Not available.
Marketing	• Public Customer Information: o Product Brochures o Owner Manuals	Limited Information available on web site. www.raisefx.com/

6. The Procedure for requesting our records

- The requester must use the prescribed form to make the request to access a record.
- This must be made to our Information Officer.
- The request must be made to our postal address, fax number or e-mail address contained herein.
- The requester must provide sufficient detail on the request form to enable the Information Officer to identify the record and the requester.
- The requester must also indicate which form of access is required and specify its postal address or fax number in the Republic.
- The requester must identify the right that is sought to be exercised or to be protected and provide an explanation as to why the requested record is required for the exercise of that right.
- If the request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the Information Officer
- The requester must use the prescribed **Form C** annexed to the manual to make the request for access to a record. This must be made to the Information Officer.
- Please see Annexure B for Form C.

7. Fees Payable for requesting our records

A requester who seeks access to a record containing personal information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee:

- The Information Officer must notify the requester (other than a personal requester) by notice, requiring the requester to pay the prescribed fee (if any) before further processing the request.
- The requester must pay a fee outlined in Annexure A. The requester may lodge an application to court against the tender or payment of the request fee.
- After the Head of our Organisation has made a decision on the request, the requester will be notified in the required form.
- If the request is granted, a further access fee must be paid for the search, reproduction, and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure.

8. Availability and updating our manual

This Manual can be viewed on our website, or is available for inspection free of charge at our above physical address. The Information Officer will update the manual on a regular basis.

9. ANNEXURE A - Fees in Respect of Private Bodies

Fees in Respect of Private Bodies

Item	Description	Amount
1.	The request fee payable by every requester	R140.00
2.	Photocopy/printed black & white copy of A4-size page	R2.00 per page or part thereof.
3.	Printed copy of A4-size page	R2.00 per page or part thereof.
4.	For a copy in a computer-readable form on:	
	(iii) Flash drive (to be provided by requestor)	R40.00
	(iv) Compact disc	
	If provided by requestor	R40.00
	If provided to the requestor	R60.00
5.	For a transcription of visual images per A4-size page Service to be outsourced. Will depend on quotation from Service provider.	
6.	Copy of visual images - Service to be outsourced. Will depend on quotation from Service provider.	
7.	Transcription of an audio record, per A4-size page	R24.00
8.	Copy of an audio record on:	
	(v) Flash drive (to be provided by requestor	R40.00
	(vi) Compact disc	
	If provided by requestor	R40.00
	If provided to the requestor	R60.00
9.	To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation. R145.00	
	To not exceed a total cost of	R435.00
10.	Deposit: If search exceeds 6 hours, a fee equal to one third of amount per request calculated in terms of items 2 to 8.	
11.	Postage, e-mail or any other electronic transfer	Actual expense, if any.”.

10. Form C

FORM C

REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))

[Regulation 11]

A. Particulars of private body

The Head:

_____

_____

_____

B. Particulars of person requesting access to the record

a)	The particulars of the person who requests access to the record must be reported below.
b)	*Furnish an address and/or fax number in the Republic to which information must be sent.*
c)	*Proof of the capacity in which the request is made, if applicable, must be attached.*

Full names and surname: _____

_____

Identity number _____

Postal address: _____

_____

_____

_____Fax number: _____

Telephone number:_____E-mail address: _____

11. Document Metadata

Document number:	**#1**
Document version:	**V1.1**
Document approval authority:	**Dany Mawas**
Document approval date:	**August 2023**
Document owner:	**Kevin Wides**
Document author(s):	**Kevin Wides**
Last updated:	**August 2023**
Next review date:	**December 2023**
Visibility (where will it be displayed):	**Website**