QUANTUM WEALTH MANAGEMENT
YOUR SUCCESS | YOUR FREEDOM | YOUR FUTURE

QUANTUM FUND MANAGERS
YOUR SUCCESS | YOUR FREEDOM | YOUR FUTURE

Quantum Wealth Management (Pty) Ltd

Registration number 2001/020621/07

FSP862 Category I and II

("the Company")

Quantum Fund Managers (Pty) Ltd

Registration number 2013/208134/07

FSP46340 Category II

("the Company")

Protection of Personal Information Policy ("the Policy")

1. Policy approval and information

Policy owner	Board of directors
Policy type	Compliance
Policy drafter	Gigi Vorlaufer
Policy reviewer	Gigi Vorlaufer
Policy creation date (1st version)	September 2019
Policy review date (this version)	May 2021
Approver's signature	
Approved by (this version)	Stefan Greeff
Adopted by (this version)	Board of directors
Approval date (this version)	July 2025
Approval date (1st version)	2020-02-12
Version number	V01.07

Summary of policy history

Version number	Drafted/adapted/reviewed by	Creation/review date	Approved by	Approval date
V01.01	Nooriah Kirsten (generic draft)	September 2019	FC Greeff	2020-02-12
V01.02	Gigi Vorlaufer (minor changes to generic draft)	November 2020	N/A	N/A
V01.03	Gigi Vorlaufer (separated from retention policy)	April 2021	N/A	N/A
V01.04	Gigi Vorlaufer (adapted for company)	May 2021	Management	May 2021
V01.05	D Kielblock	March 2023	Management	March 2023
V01.06	S Greeff	October 2023	Management	October 2023
V01.07	Gigi Vorlaufer & Stefan Greeff (template compliance integration)	July 2025	Stefan Greeff	July 2025

2. Protection of Personal Information

2.1. Purpose and scope

The Protection of Personal Information policy is prescribed in terms of the Protection of Personal Information Act 4 of 2014 (the POPIA), as amended or substituted from time to time. The right to privacy is an integral human right recognised and protected in the South African Constitution and in the POPIA. The POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of Personal Information, in a context-sensitive way.

The Company, either directly, or via its subsidiaries, is authorised/licensed/registered in terms of the following financial sector laws:

- Authorised Financial Services Provider ("FSP"), licensed under the Financial Advisory and Intermediary Services Act 37 of 2002 ("the FAIS Act")
    - FSP: 862 (QWM); 46340 (QFM)

- Manager of collective investment schemes ("CIS manager"), licensed under the Collective Investment Schemes Control Act 45 of 2002 ("the CISCA")

- Accountable institution, registered under the Financial Intelligence Centre Act 38 of 2001 ("the FICA")
    - Organisation number: QWM: AI/110218/00115 & QFM: XXXX

Through the providing of these services, the Company is necessarily involved in collecting, using and disclosing certain aspects of the Personal Information of its clients, employees and other stakeholders. As a Responsible Party, the Company must comply with the POPIA. The POPIA requires the Company to inform its clients about the way their Personal Information is used, disclosed and destroyed.

A person's right to privacy entails having control over their Personal Information and being able to conduct their affairs relatively free from unwanted intrusions. Given the importance of privacy, the Company is committed to effectively managing Personal Information in accordance with the POPIA. The Company is committed to protecting the privacy of its clients and ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out the way the Company deals with its clients' Personal Information and stipulates the purpose for which the information is used and how it is used. The Policy is made available on the company website (www.quantumam.co.za) and by request, from the Company head office.

This Policy must be read together with:

- Retention of Documents Policy, in terms of the Protection of Personal Information Act 4 of 2013 ("POPIA")
- Information Security and Privacy Policy, in terms of the Electronic Communications and Transactions Act 25 of 2002 ("ECTA")
- PAIA Manual, in terms of the Promotion of Access to Information Act 2 of 2000 ("PAIA")

The purpose of this Policy is to:

2.1.1. protect the Company from the compliance risks associated with the protection of Personal Information, which includes:

- breaches of confidentiality
- reputational damage

2.1.2. demonstrate the Company's commitment to protecting the privacy rights of Data Subjects:

- through stating desired behaviour and directing compliance with the provisions of the POPIA and best practice
- by cultivating a culture that recognises privacy as a valuable human right
- by developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of Personal Information
- by creating business practices that will provide reasonable assurance that the rights of Data Subjects are protected and balanced with the legitimate business needs of the Company
- by assigning specific duties and responsibilities to control owners including the appointment of an Information Officer and where necessary, Deputy Information Officers, to protect the interests of the Company and Data Subjects;
- by raising awareness through training and providing guidance to individuals who process Personal Information so that they can act confidently and consistently.

2.2. Legislative framework

Any reference to legislation, subordinate legislation and supervision documents, includes amendments made from time to time. The legislative framework comprises, among others, the following:

- Collective Investment Schemes Control Act 45 of 2002 ("the CICSA")
- Companies Act 71 of 2008 ("the CA")
- Conduct of Financial Institutions Bill ("the COFI Bill")
- Constitution of the Republic of South Africa, 1996 ("the Constitution")
- Cybercrime Act 19 of 2020 ("the Cybercrime Act")
- Electronic Communications and Transactions Act 25 of 2002 ("the ECTA")
- Exchange Control Regulations, as published by the South African Reserve Bank ("the Excon regulations")
- Financial Advisory and Intermediary Services Act 37 of 2002 ("the FAIS Act")
- Financial Intelligence Centre Act 38 of 2001 ("the FICA")
- Financial Markets Act 19 of 2012 ("the FMA")
- Financial Sector Regulation Act 9 of 2017 ("the FSRA")
- Friendly Societies Act 25 of 1956 ("the FS Act")
- Income Tax Act 58 of 1962 ("the ITA")
- Pension Funds Act 24 of 1956 ("the PFA")
- Prevention and Combating of Corrupt Activities Act 12 of 2004 ("the Prevention Act")
- Prevention of Organised Crime Act 121 of 1998 ("the POCA")
- Promotion of Access to Information Act 2 of 2000 ("the PAIA")
- Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 ("the POCDATARA Act")
- Protection of Personal Information Act 4 of 2013 ("the POPIA")
- Value-Added Tax Act 89 of 1991 ("the VAT Act")

2.3. Definitions

2.3.1. **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.

2.3.2. **Child** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person to take any action or decision in respect of any matter concerning himself or herself

2.3.3. **Competent Person** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child (i.e. the child's legal guardian)

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

2.3.5. **Data Subject** means the person to whom **Personal Information** relates

2.3.6. **De-identify** and **de-identified** in relation to Personal Information of a **Data Subject**, means to delete, or replace any information that:

- identifies the Data Subject
- can be used or manipulated by a reasonably foreseeable method to identify the Data Subject
- can be linked by a reasonably foreseeable method to other information that identifies the Data Subject

2.3.7. **Direct marketing** means to approach a Data Subject either in person or by mail or electronic communication for the direct or indirect purpose of:

- promoting or offering to supply, in the ordinary course of business, any goods or services to the Data Subject
- requesting the Data Subject to make a donation of any kind for any reason

2.3.8. **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

2.3.9. **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

2.3.10. **Head of a private body** means:

- in the case of a natural person, that natural person or any person duly authorised by that natural person
- in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership
- in the case of a **juristic person**:
    - the **chief executive officer** or equivalent officer of the juristic person or **any person duly authorised by that officer**
    - the person who is acting as such or any person duly authorised by such acting person

2.3.11. **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 (10) or more, Data Subjects, with one (1) or more, documents that contain Personal Information of ten (10) 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

2.3.12. **Information officer** of or in relation to, a:

- **public body** means an Information Officer or Deputy Information Officer, as contemplated in terms of section 1 or 17 of the **PAIA**
- **private body** means the **head of a private body**, as contemplated in section 1 of the PAIA

2.3.13. **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

2.3.14. **Person** means a natural person or a juristic person

2.3.15. **Personal Information** means information about an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- information about 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
- information relating to the education or the medical, financial, criminal or employment history of the person
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- the biometric information of the person
- the personal opinions, views or preferences of the person
- 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
- the views or opinions of another individual about the person
- the name of the person if it appears with other Personal Information about the person or if the disclosure of the name itself, would reveal information about the person

2.3.16. **Private body** means:

- a natural person who carries or has carried on any trade, business or profession, but only in the capacity as a natural person
- a partnership which carries or has carried on any trade, business or profession
- any former or existing **juristic person, but excludes a public body**

2.3.17. **Processing** means any operation or activity or any set of operations, whether or not, by automatic means, about Personal Information including:

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

- dissemination by means of transmission, distribution or making available in any other form
- merging, linking and restriction, degradation, erasure or destruction of information

2.3.18. **Public body** means:

- any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government
- any other functionary or institution when:
  - exercising a power or performing a duty in terms of the Constitution or a provincial constitution
  - exercising a public power or performing a public function in terms of any legislation

2.3.19. **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

2.3.20. **Record** means any recorded information:

- regardless of form or medium including:
  - writing on any material
  - 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 produced, recorded or stored
  - label, marking or other writing that identifies or describes anything of which it forms part or to which it is attached by any means
  - book, map, plan, graph or drawing
  - photograph, film, negative, tape or other device, in which one (1) or more visual images are embodied to be capable with or without the aid of some other equipment of being reproduced
- in the possession or under the control of a Responsible Party
- whether or not it was created by a Responsible Party

- regardless of when it came into existence

2.3.21. **Regulator** means the Information Regulator established in terms of section 39 of the POPIA

2.3.22. **Re-identify** and **re-identified** in relation to Personal Information of a Data Subject, means to resurrect any information that has been de-identified that:

- identifies the Data Subject
- can be used or manipulated by a reasonably foreseeable method to identify the Data Subject
- can be linked by a reasonably foreseeable method to other information that identifies the Data Subject

2.3.23. **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

2.3.24. **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 the information

2.3.25. **Special Personal Information** means Personal Information as referred to in section 26 of the POPIA:

- religious or philosophical, beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject
- criminal behaviour of a Data Subject to the extent that the information relates to:
    - alleged commission by a Data Subject of any offence
    - proceedings about any offence allegedly committed by a Data Subject or the disposal of those proceedings

2.3.26. **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 for that Responsible Party.

2.3.27. **Automated decision-making** means a decision that is based solely on automated processing of personal information intended to provide a profile of a person, including their performance at work, creditworthiness, reliability, location, health, personal preferences, or conduct, and that produces legal effects or significantly affects the data subject.

2.3.28. **Data subject participation** refers to the right of a data subject to access, correct, delete, or object to the processing of their personal information, as set out in Chapter 3, Part C of the POPIA.

2.4. Lawful processing of Personal Information

2.4.1. The Company as the Responsible Party or as the Operator MUST adhere to the 8 conditions for the lawful processing of Personal Information:

- Condition 1: Accountability
- Condition 2: Processing limitation
- Condition 3: Purpose specification
- Condition 4: Further processing limitation
- Condition 5: Information quality
- Condition 6: Openness
- Condition 7: Security safeguards
- Condition 8: Data Subject participation

2.5. Condition 1: Accountability – Responsible Party to ensure conditions for lawful processing

2.5.1. The Company as the Responsible Party, must ensure that it complies with the conditions and the measures that give effect to the conditions when it determines the purpose of processing, how it processes and during the processing.

2.5.2. Where the Company is acting as the Operator, the Responsible Party must ensure that the Company complies with the relevant conditions and the measures that give effect to the conditions, when it determines the purpose of processing, how it processes and during the processing.

2.6. Condition 2: Processing limitation – lawfulness of processing

2.6.1. The Company MUST only process Personal Information lawfully and reasonably in a way that does not infringe the privacy of the Data Subject.

2.7. Condition 2: Processing limitation - minimality

2.7.1. The Company may only process Personal Information that is adequate, relevant and not excessive based on the purpose for processing that information.

2.7.2. The Company collects and processes Data Subjects' Personal Information in terms of several other laws, associated with the functions performed by the Company, including the FAIS Act and the FICA. As an FSP, providing financial advice and non-discretionary intermediary services in terms of FAIS, the Company obtains Personal Information of potential and existing clients to determine the client's financial needs and investment objectives. An FSP is also an AI in terms of the FICA, which must perform initial and ongoing customer due diligence processes. This includes establishing and verifying the identity of the potential and existing client, the beneficial owners and other persons associated with the business relationship and includes performing screening searches, to determine the riskiness of the client and the overall business relationship. The type of information depends on the purpose for which it is collected and will be processed for that purpose only. Wherever possible, the Company will inform the client about the information required and the information deemed optional.

2.7.3. Employees of the Company are also Data Subjects and the Company collects Personal Information of potential and existing employees in terms of other laws, including the FAIS Act and employment laws.

2.7.4. Examples of Personal Information that the Company collects from Data Subjects includes:

- Identity number, passport number, date of birth, nationality, full name physical and postal addresses, marital status, income tax number, number of dependants, race, gender
- Description of residence, business, assets, liabilities, financial information, banking details
- Qualifications, education, employment history, criminal history, credit history
- Any other information required by the Company, its product suppliers, third party service providers

2.7.5. The Company also collects and processes clients' Personal Information for marketing purposes to ensure that our financial products and services remain relevant to our clients and potential clients.

2.7.6. From the effective date of the regulations to the POPIA, if the Company wants to engage in direct marketing, it must use the prescribed Form 4, as contained in the regulations, to apply for the consent of a Data Subject, for processing Personal Information for the purpose of direct marketing.

2.7.7. The Company aims to have agreements in place with all product suppliers, other FSPs and third-party service providers, to ensure a mutual understanding regarding the protection of clients' Personal Information. The Company's product suppliers will be subject to the same regulations, as applicable to the Company, in terms of the protection of clients' Personal Information.

2.8. Condition 2: Processing limitation – consent, justification and objection

2.8.1. The Company MAY ONLY process Personal Information IF the:

- **Data Subject** or a competent person (only where the Data Subject is a child), **consents to the processing**. For example, consent is obtained from clients

during the introductory appointment and needs analysis, stage of the business relationship

- processing is necessary to carry out actions for the conclusion or performance, of a **contract to which the Data Subject is party**. For example, to conduct an accurate analysis of the client's financial needs and objectives
- processing **complies with an obligation imposed by law on the Responsible Party**. For example, as required by the FAIS Act, the FICA, employment related legislation, tax related legislation
- processing **protects a legitimate interest of the Data Subject**. For example, it is in the client's best interest to have a full and proper, financial needs analysis performed, to provide them with an applicable and beneficial, financial product or financial service
- processing is necessary for **pursuing the legitimate interests of the Company or third-parties, to whom the information is supplied**. For example, to provide the Company's clients with financial products or financial services, the Company, its product suppliers, its service providers and other relevant third parties, require certain Personal Information from the clients, to make an expert decision about the unique and specific, financial product or financial service, required.

2.8.2. The Company must classify all the Personal Information processed, according to the reasons for which Personal Information is processed, to ensure that it only processes Personal Information for permitted reasons and to identify the instances where the Data Subject may object to the processing of their Personal Information.

2.8.3. If the Company identifies that it is processing Personal Information for a reason that is not a permitted reason, it must take corrective action.

2.8.4. The Company, as the Responsible Party, MUST have proof of the Data Subject's consent, where consent is required.

2.8.5. Where the Company is acting as the Operator, the Responsible Party MUST ensure that it provides the Company with the proof of the Data Subject's consent, where consent is required.

2.8.6. Where the Data Subject's consent for processing their Personal Information is required, the Company MUST allow the Data Subject to withdraw their consent, at any time, as long as the lawfulness of the processing before the withdrawal of consent or the processing, where consent is not required, will not be affected by the withdrawal of consent.

2.8.7. If a Data Subject objects to the processing of their Personal Information (using the prescribed Form 1 and on reasonable grounds relating to their situation), where the reason for the processing:

- protects a legitimate interest of the Data Subject
- processing is necessary for the proper performance of a public law duty by a public body
- processing is necessary for pursuing the legitimate interests of the Responsible Party
- processing is necessary for pursuing the legitimate interests of a third party to whom the information is supplied,

2.9. Condition 2: Processing limitation – collection directly from Data Subject

2.9.1. The Company MUST collect Personal Information directly from the Data Subject, except if:

- information is contained in or derived from, a public record or has deliberately been made public by the Data Subject
- **Data Subject or a competent person (only where the Data Subject is a child), consents to the collection of the information from another source**
- **collection of the information from another source would not prejudice a legitimate interest of the Data Subject**
- collection of the information from another source is necessary:
    - to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment, of offences

- **to comply with an obligation imposed by law** or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
- for the conduct of proceedings in any court or tribunal, which have commenced or are reasonably contemplated
- in the interests of national security
- to maintain the legitimate interests of the Responsible Party
- to maintain the legitimate interests of a third party to whom the information is supplied

- **compliance would prejudice a lawful purpose of the collection**
- **compliance is not reasonably practicable in the circumstances of the case**.

2.10. Condition 3: Purpose specification - collection for specific purpose

2.10.1. The Company MUST only collect Personal Information of Data Subjects for the specific, explicitly defined and lawful, purpose, based on the relevant function or activity, of the Company, where it is the Responsible Party or based on the relevant function or activity of the Responsible Party, where the Company is acting as the Operator.

2.11. Condition 3: Purpose specification - retention and restriction of records

2.11.1. The Company MUST NOT retain records of Personal Information for any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, UNLESS:

- retention of the record is required or authorised, by law
- the Responsible Party reasonably requires the record for lawful purposes, related to its functions or activities
- retention of the record is required by a contract between the parties thereto
- the Data Subject or a competent person (only where the Data Subject is a child), consents to the retention of the record.

2.11.2. The Company MUST determine and should document, in the **Retention of documents policy** (forming part of this Policy), the maximum document retention timeframes necessary for achieving the purpose for which the information was collected or subsequently processed.

2.11.3. The Company MAY retain records of Personal Information for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, FOR historical, statistical or research, purposes, IF the Responsible Party has established appropriate safeguards against the records being used for any other purposes.

2.11.4. Where the Company is acting as the Responsible Party and retains records of Personal Information for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, FOR historical, statistical or research, purposes, it MUST establish appropriate safeguards against the records being used for any other purposes.

2.11.5. Where the Company is acting as the Operator and retains records of Personal Information for longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, FOR historical, statistical or research, purposes, the Responsible Party must ensure that it establishes and provides the Company with, appropriate safeguards against the records being used for any other purposes.

2.11.6. Where the Company, as the Responsible Party or acting as the Operator, has used a record of Personal Information of a Data Subject to decide about the Data Subject, IT MUST:

- retain the record for the period, as may be required or prescribed, by law or a code of conduct
- if there is no law or code of conduct, prescribing a retention period, retain the record for a period that will afford the Data Subject a reasonable opportunity, taking all considerations about the use of the Personal Information into account, to request access to the record.

2.11.7. The Company, as the Responsible Party, MUST destroy or delete, a record of Personal Information or de-identify it, as soon as reasonably practicable after the Company is no longer authorised to retain the record.

2.11.8. Where the Company acts as the Operator, on behalf of the Responsible Party, the Responsible Party must ensure that the Company is instructed to destroy or delete, a record of Personal Information or de-identify it, as soon as reasonably practicable after the Responsible Party is no longer authorised to retain the record.

2.11.9. When the Company destructs or deletes, a record of Personal Information, IT MUST be done in a way that prevents its reconstruction in an intelligible form.

2.11.10. The Company, as the Responsible Party, MUST restrict processing of Personal Information, IF:

- its accuracy is contested by the Data Subject, for long enough to enable the Company to verify the accuracy of the information
- the Company no longer needs the Personal Information to achieve the purpose for which the information was collected or subsequently processed, but it MUST be maintained for purposes of proof
- the processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use
- the Data Subject requests to transmit the personal data into another automated processing system.

2.11.11. Where the Company is acting as the Operator, the Responsible Party must ensure that the Company restricts the processing of Personal Information, when required.

2.11.12. Where processing of Personal Information is restricted, the Company MUST ONLY process the Personal Information (except for storage):

- for purposes of proof
- with the Data Subject's consent or a competent person (only where the Data Subject is a child)

- for the protection of the rights of another person
- if the processing is in the public interest

2.11.13. Where processing of Personal Information is restricted and the Company is the Responsible Party, the Company MUST inform the Data Subject BEFORE lifting the restriction on processing.

2.11.14. Where processing of Personal Information is restricted and the Company is acting as the Operator, the Responsible Party MUST inform the Data Subject BEFORE lifting the restriction on processing.

2.12. Condition 4: Further processing limitation - further processing to be compatible with purpose of collection

2.12.1. Where the Company performs further processing of Personal Information, it MUST be according to or compatible with, the specific, explicitly defined and lawful, purpose for which it was collected, which relates to a function or activity, of the Company, where it is the Responsible Party or relates to a function or activity of the Responsible Party, where the Company is acting as the Operator, on behalf of the Responsible Party.

2.12.2. Where the Company is the Responsible Party, IT MUST assess whether further processing is compatible with the purpose of collection, by considering the:

- relationship between the purpose of the intended further processing and the purpose for which the information was collected
- nature of the information concerned
- consequences of the intended further processing for the Data Subject
- way the information was collected
- contractual rights and obligations, between the parties.

2.12.3. Where the Company is acting as the Operator, the Responsible Party must ensure that the Company considers the required aspects, when it assesses whether further processing is compatible with the purpose of collection.

2.12.4. When the Company is assessing whether further processing is compatible with the purpose of collection, it may consider the following aspects to be compatible:

- the Data Subject or a competent person (only where the Data Subject is a child), consents to the further processing of the information
- the information is available in or derived from, a public record or has deliberately been made public by the Data Subject
- further processing is necessary:
    - to avoid prejudice to the maintenance of the law, by any public body, including the prevention, detection, investigation, prosecution and punishment, of offences
    - to comply with an obligation imposed by law or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
    - for the conduct of proceedings in a court or tribunal, which have commenced or are reasonably contemplated
    - in the interests of national security
- the further processing of the information is necessary to prevent or mitigate, a serious and imminent, threat to:
    - public health or public safety
    - the life or health, of the Data Subject or another individual
- the information is used for historical, statistical or research, purposes and the Responsible Party ensures that the further processing is carried out solely for those purposes and will not be published in an identifiable form
- the further processing of the information is according to an exemption granted by the Regulator.

2.13. Condition 5: Information quality - quality of information

2.13.1. The Company, as the Responsible Party, MUST take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated, where necessary, based on the purpose for which the Personal Information is collected or further processed.

2.13.2. Where the Company is acting as the Operator, the Responsible Party must ensure that the Company takes reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated, where necessary, based on the purpose for which the Personal Information is collected or further processed.

2.14. Condition 6: Openness – Documentation

2.14.1. The Company, as the Responsible Party, MUST maintain the documents of all processing operations that it is responsible for and which information must be included in the PAIA manual, relating to the:

- purpose of the processing
- description of the categories of Data Subjects and of the information or categories of information, relating thereto
- recipients or categories of recipients, to whom the Personal Information may be supplied
- planned transborder flows of Personal Information
- general description, allowing a preliminary assessment of the suitability of the information security measures to be implemented by the Company, to ensure the confidentiality, integrity and availability, of the information that is to be processed.

2.14.2. The Company MUST update its PAIA manual, to include the required information for protecting Personal Information and publish the updated manual, as required.

2.14.3. Where the Company is acting as the Operator, the Responsible Party must ensure that the Company maintains the required documents of all processing operations that it is responsible for.

2.15. Condition 6: Openness – notification to Data Subject when collecting Personal Information

2.15.1. The Company, as the Responsible Party, MUST ensure that the Data Subject is aware of the:

- information that is collected
- source from which the information is collected, where the information is not collected directly from the Data Subject
- name and address, of the Company, as the Responsible Party
- purpose for collecting the information
- fact that the information they supply is either voluntary or mandatory
- consequences of failing to provide the information
- law authorising or requiring, the collecting of the information
- fact that, where applicable, the Company, as the Responsible Party, intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation
- other relevant information, which is necessary, in the specific circumstances in which the information is or is not, to be processed, to enable processing, for the Data Subject, to be reasonable, such as:
    - recipient or category of recipients, of the information
    - nature or category, of the information
    - existence of the right of access to and the right to rectify, the information collected
    - existence of the right to object to the processing of Personal Information
    - right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator

2.15.2. The Company, as the Responsible Party, MUST make the Data Subject aware of the required information, BEFORE the Personal Information is collected, IF it is collected directly from the Data Subject, UNLESS the Data Subject is already aware of the required information.

2.15.3. The Company, as the Responsible Party, MUST make the Data Subject aware of the required information, BEFORE the Personal Information is collected or as soon as

reasonably practicable after it has been collected, IF it is NOT collected directly from the Data Subject.

2.15.4. Where the Company, as the Responsible Party, has previously made the Data Subject aware of the required information, IT complies with the awareness requirement, for subsequent collection, from the Data Subject, of the same information or information of the same kind, IF the purpose of collection of the information remains the same.

2.15.5. Where the Company is acting as the Operator, the Responsible Party must ensure that the Data Subject is aware of the required information, within the prescribed timeframe.

2.15.6. The Company, as the Responsible Party or acting as the Operator, **DOES NOT need to comply with the awareness requirement, IF:**

- Data Subject or a competent person (only if the Data Subject is a child), consents to the non-compliance
- non-compliance would not prejudice the legitimate interests of the Data Subject
- non-compliance is necessary:
    - to avoid prejudice to the maintenance of the law, by a public body, including the prevention, detection, investigation, prosecution and punishment, of offences
    - to comply with an obligation imposed by law or to enforce legislation about the collection of revenue (in terms of the South African Revenue Service Act)
    - for the conduct of proceedings in a court or tribunal, which have been commenced or are reasonably contemplated
    - in the interests of national security
- compliance would prejudice a lawful purpose of the collection
- compliance is not reasonably practicable in the circumstances of the case
- information will:
    - not be used in a form in which the Data Subject may be identified
    - be used for historical, statistical or research, purposes.

2.15.7. The Company collects and further processes, information of clients, as Data Subjects, for functions or activities, including, but not limited to:

- Performing the initial and ongoing, customer due diligence reviews, for the client and other people involved in the business relationship
- Assigning a unique identifier to clients (client number)
- Providing financial products or financial services to clients, carrying out the instructions and transactions, related thereto
- Collecting, further processing and reporting, information about the tax residency of clients
- Underwriting
- Assessing and processing, claims
- Confirming, verifying and updating, information
- Claims history
- Detecting and preventing, fraud, crime, money laundering or other unlawful activities
- Screening of United Nations lists
- Determining the riskiness of clients, other people involved in the business relationship and the business relationship
- Conducting market or client, satisfaction research
- Audit and record keeping
- Legal proceedings
- Activities relating to maintaining and improving, the business relationship
- Providing communication about the Company, its financial products, the underlying financial products and financial services and regulatory matters, which may affect clients
- Sharing information with other relevant FSPs, product suppliers and service suppliers, with whom we have business relationships, to process information on our behalf or to those who provide services to us
- Complying with legal and regulatory requirements or when it is otherwise allowed by law.

2.15.8. The Company collects and further processes, information of employees, as Data Subjects, for functions or activities, including, but not limited to:

- Determining the fitness and propriety, of the person
- Confirming, verifying and updating, information, including aspects such as qualifications, education, employment history, criminal history, credit history
- Detecting and preventing, fraud, crime, money laundering or other unlawful activities
- Legal proceedings
- Audit and record keeping
- Sharing information with other relevant FSPs, product suppliers and service suppliers, with whom we have business relationships, to process information on our behalf or to those who provide services to us
- Complying with, legal and regulatory requirements or when it is otherwise allowed by law.

2.16. Condition 7: Security safeguards - security measures on integrity and confidentiality of Personal Information

2.16.1. The Company, as the Responsible Party or acting as the Operator, MUST secure the integrity and confidentiality, of Personal Information in its possession or under its control, by taking appropriate, reasonable, technical and organisational, measures to prevent:

- loss of, damage to or unauthorised destruction of, Personal Information
- unlawful access to or processing of, Personal Information,

by taking reasonable measures to:

- identify all reasonably foreseeable internal and external, risks to Personal Information in its possession or under its control
- establish and maintain, appropriate safeguards against the risks identified
- regularly verify that the safeguards are effectively implemented
- ensure that the safeguards are continually updated, in response to new risks or deficiencies in previously implemented safeguards.

2.16.2. Where the Company is acting as the Operator, the Responsible Party must ensure that the Company secures the integrity and confidentiality, of Personal Information in its possession or under its control, by taking appropriate, reasonable, technical and organisational, measures.

2.16.3. The Company, as the Responsible Party, MUST have due regard to generally accepted information security practices and procedures, which may apply to it, generally or be required in terms of specific industry or professional, rules and regulations.

2.16.4. Where the Company is acting as the Operator, on behalf of the Responsible Party, the Responsible Party must ensure that the Company has due regard to generally accepted information security practices and procedures, which may apply to it, generally or be required in terms of specific industry or professional, rules and regulations.

2.17. Condition 7: Security safeguards - information processed by Operator or person acting under authority

2.17.1. Where the Company is acting as the Operator, IT MUST:

- only process the information with the knowledge or authorisation, of the Responsible Party
- treat Personal Information that comes to its knowledge, as confidential and must not disclose it,

unless required by law or during the proper performance of its duties.

2.18. Condition 7: Security safeguards - security measures regarding information processed by Operator

2.18.1. Where the Company is acting as the Operator, the Responsible Party must, in terms of the written contract between the Responsible Party and the Company, ensure that the Company establishes and maintains, the required security measures.

2.18.2. Where the Company is acting as the Operator, IT MUST notify the Responsible Party immediately, where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired, by any unauthorised person.

2.19. Condition 7: Security safeguards - notification of security compromises

2.19.1. Where the Company is the Responsible Party and there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired, by any unauthorised person, it MUST NOTIFY (in writing):

- Regulator
- Data Subject, unless the identity of the Data Subject cannot be established,

as soon as reasonably possible, after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Company's information system.

2.19.2. The Company, as the Responsible Party, may only delay notifying the Data Subject, IF a public body, responsible for the prevention, detection or investigation, of offences or the Regulator, determines that notification will impede a criminal investigation, by the public body.

2.19.3. Where the Company is acting as the Operator, IT MUST immediately notify the Responsible Party and provide the Responsible Party with the required information, so the Responsible Party can notify the Regulator and the Data Subject.

2.19.4. The Company MUST notify, in writing, the Data Subject, about a Personal Information compromise, in at least one (1) of the following ways:

- mailed to the Data Subject's last known physical or postal, address
- sent by e-mail to the Data Subject's last known e-mail address
- placed in a prominent position on the website of the Responsible Party
- published in the news media
- as may be directed by the Regulator.

2.19.5. The Company MUST ensure that the notification to the Data Subject provides sufficient information to allow the Data Subject to take protective measures against the potential consequences of the Personal Information compromise, including:

- description of the possible consequences of the security compromise
- description of the measures that the Responsible Party intends to take or has taken, to address the security compromise
- recommendation about the measures to be taken by the Data Subject, to mitigate the possible adverse effects of the security compromise
- if known to the Responsible Party, the identity of the unauthorised person, who may have accessed or acquired, the Personal Information.

2.19.6. The Company, as the Responsible Party, MUST publicise, in a way specified by the Regulator, a Personal Information compromise, if directed to do so, by the Regulator.

- The Regulator will direct a Responsible Party to publicise a personal data compromise, if it has reasonable grounds to believe that the publicity would protect a Data Subject, who may be affected by the compromise.

2.20. Condition 8: Data Subject participation – access to Personal Information

2.20.1. A Data Subject that provides the Company with adequate proof of identity, may ask the Company, as the Responsible Party, to confirm, free of charge, whether or not, the Company holds Personal Information about the Data Subject.

2.20.2. A Data Subject that provides the Company with adequate proof of identity, may ask the Company, as the Responsible Party, for the record or a description, of the Personal Information about the Data Subject, held by the Company, including information about the identity of all third parties or categories of third parties, who have or have had, access to the information:

- within a reasonable time
- at a prescribed fee, if any
- in a reasonable way and format
- in a form that is generally understandable.

2.20.3. If the Company communicates Personal Information to a Data Subject, in response to a request from the Data Subject, it MUST advise the Data Subject of their right to request their Personal Information to be corrected.

2.20.4. If the Company, as the Responsible Party, requires a Data Subject making a request, to pay a fee for services provided to the Data Subject, to enable the Responsible Party to respond to a request, the Company:

- must give the applicant a written estimate of the fee, before providing the services
- may require the applicant to pay a deposit for all or part, of the fee.

2.20.5. The Company, as the Responsible Party, MAY or MUST, refuse, as the case may be, to disclose information requested by the Data Subject, to which the grounds for refusal of access to records are set out in the applicable sections of the PAIA.

- **Refer to the PAIA manual for details.**

2.20.6. The Company, as the Responsible Party, must apply the applicable provisions of the PAIA, for access to health or other, records.

- **Refer to the PAIA manual for details.**

2.20.7. Where a Data Subject requests access to Personal Information and part of that information MAY or MUST, be refused, in terms of the PAIA, the Company MUST disclose all other parts of the requested information.

2.20.8. The Company will take reasonable steps to confirm a Data Subject's identity, before providing details of their Personal Information.

2.21. Condition 8: Data Subject participation – correction of Personal Information

2.21.1. A Data Subject may, using the prescribed Form 2, request the Company, as the Responsible Party, to:

- correct or delete, Personal Information about the Data Subject, in its possession or under its control, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully
- destroy or delete, a record of Personal Information about the Data Subject, which the Company, as the Responsible Party, is no longer authorised to retain, because it is no longer necessary for achieving the purpose for which the information was collected or subsequently processed

2.21.2. Where the Company, as the Responsible Party, receives a request to correct or delete, Personal Information, it MUST, as soon as reasonably practicable:

- correct the information
- destroy or delete, the information
- provide the Data Subject, to their satisfaction, with credible evidence, in support of the information
- where agreement cannot be reached between the Company and the Data Subject and if the Data Subject requests, take steps that are reasonable, in the circumstances, to attach to the information in a way that it will always be read with the information, an indication that a correction of the information has been requested, but has not been made

2.21.3. Where the Company, as the Responsible Party, has taken steps that result in a change to the Data Subject's Personal Information and the changed information has an impact on decisions that have been or will be, taken in respect of the Data Subject in question, it MUST, if reasonably practicable, inform each person or body or Responsible Party, to whom the Personal Information has been disclosed of those steps.

2.21.4. The Company, as Responsible Party, MUST notify a Data Subject, who has made a request to correct or delete, their Personal Information, of the action taken, due to the request.

2.21.5. The Company will take reasonable steps to confirm a Data Subject's identity, before correcting or deleting, their Personal Information.

2.22. Condition 8: Data Subject participation – manner of access

2.22.1. The Company MUST consider that the provisions of the PAIA, about the form of requests, apply to requests for access to Personal Information.

- **Refer to the PAIA manual for details.**

2.22.2. The Company should ensure that requests from Data Subjects are received, using the prescribed forms, for the type of request, as prescribed by the Regulator.

2.23. Processing of special Personal Information

2.23.1. The Company, as the Responsible Party, **MAY NOT process Personal Information about**:

- religious or philosophical, beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex, life or biometric information, of a Data Subject
- criminal behaviour of a Data Subject, to the extent that the information relates to:
  - alleged commission by a Data Subject, of an offence
  - proceedings about an offence allegedly committed by a Data Subject or the disposal of the proceedings,

UNLESS the prohibition on processing special Personal Information does not apply.

2.23.2. The Company must be aware that the prohibition on processing special Personal Information DOES NOT APPLY, IF the:

- processing is carried out with the consent of a Data Subject
- processing is necessary for the establishment, exercise or defence, of a right or obligation, in law
- processing is necessary to comply with an obligation of international public law
- processing is for historical, statistical or research, purposes, to the extent that:
  - purpose serves a public interest and the processing is necessary for the purpose concerned
  - it appears to be impossible or would involve a disproportionate effort, to ask for consent,

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

- information has deliberately been made public by the Data Subject
- provisions applicable to obtaining authorisation about a Data Subject's religious or philosophical, beliefs or criminal behaviour or biometric information, are complied with, as applicable to the case.

2.23.3. The Company, as the Responsible Party, may apply to the Regulator, to process special Personal Information, if the processing is in the public interest and if appropriate safeguards have been put in place, to protect the Personal Information of the Data Subject.

- The Regulator may approve the application, but may impose reasonable conditions related to the authorisation.

2.23.4. The Company may process Personal Information about a **Data Subject's race or ethnic origin, IF** the processing is carried out to:

- identify Data Subjects and **only when this is essential to identify Data Subjects**; AND
- comply with laws and other measures, designed to **protect or advance, persons or categories of persons, disadvantaged by unfair discrimination**.

2.23.5. The Company may process Personal Information about a **Data Subject's health or sex life**, provided it renders services only in specific and relevant sectors where such information is necessary.

2.23.6. Quantum does not render services in those specific sectors and therefore do not process personal information about your health and or sex life. Note however in some instances where we act as your advisor for certain risk insurance related products, such insurers may require health and related information from you.

2.23.7. Where the Company may process Personal Information about a Data Subject's health or sex life, the information may only be processed by Responsible Parties, subject to an obligation of confidentiality, by virtue of office, employment, profession or legal provision, or established by a written agreement between the Responsible Party and the Data Subject.

2.23.8. Where the Company may process information about a Data Subject's health or sex life and is not subject to an obligation of confidentiality, by virtue of office, profession or legal, provision, it must treat the information as confidential, unless it is required by law or in connection with its duties to communicate the information to other parties, who are authorised to process the information.

2.23.9. The prohibition on processing any of the categories of special Personal Information, does not apply, IF it is necessary to supplement the processing of Personal Information about a Data Subject's health, with a view to the proper treatment or care, of the Data Subject.

2.23.10. Personal Information about inherited characteristics may not be processed for a Data Subject from whom the information has been obtained, UNLESS:

- a serious medical interest prevails; or
- the processing is necessary for historical, statistical or research, activity.

2.23.11. The Company may process Personal Information about a **Data Subject's criminal behaviour or biometric information, IF** it is a Responsible Party, who has obtained the information in accordance with the law.

2.23.12. Where the Company may process Personal Information about its **employees' criminal behaviour or biometric information**, it must be done in accordance with the rules established in compliance with labour legislation.

2.23.13. The prohibition on processing any of the categories of special Personal Information, does not apply, IF it is necessary to supplement the permitted processing of information about criminal behaviour or biometric information.

Note: The Company does not engage in decisions that produce legal effects concerning a data subject based solely on automated processing of personal information. If this changes, data subjects will be informed and given the opportunity to object or request human intervention.

2.24. Processing of Personal Information of children

2.24.1. The Company, as the Responsible Party, **MAY NOT process Personal Information of children**,
UNLESS the prohibition on processing the Personal Information of children does not apply.

2.24.2. The Company, as the Responsible Party, **MAY process Personal Information of children, IF** it is:

- **carried out with the prior consent of the legal guardian** (competent person);
- necessary to establish, exercise or defend, a right or obligation, in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research, purposes, to the extent that:
    - the purpose serves a public interest and the processing is necessary for the purpose concerned;
    - it appears to be impossible or would involve a disproportionate effort, to ask for consent,

  and sufficient guarantees are provided for, to ensure that the processing does not adversely affect the individual privacy of the child, to a disproportionate extent;
- Personal Information, which has deliberately been made public by the child, with the consent of the legal guardian (competent person).

2.24.3. The Company will obtain consent from the competent person (legal guardian) of children, BEFORE processing children's information.

2.25. Prior authorisation

2.25.1. The Company, as the Responsible Party, **WILL OBTAIN prior authorisation from the Information Regulator BEFORE processing**, **IF it ever plans to**:

- process any **unique identifiers** of Data Subjects:
  - for purposes other than the purpose for which the unique identifier was specifically intended at collection; **AND**
  - with the aim of linking the information, together with information processed by other Responsible Parties;
- process information on **criminal behaviour or on unlawful or objectionable, conduct, on behalf of third parties**;
- process information for the purposes of **credit reporting**; or
- transfer special Personal Information or the Personal Information of children, to a third party, in a foreign country that does not provide an adequate level of protection for the processing of Personal Information.

2.25.2. As part of its normal business processes, the Company does not process Personal Information for the affected purposes.

2.25.3. Through the information officer, the Company **WILL** keep informed about potential changes to the processing of specific types of personal information that require the prior authorisation from the information regulator. If required, it will submit an application to the information regulator, to obtain prior authorisation to process the affected personal information.

2.25.4. If the Company, as the responsible party, is processing information that requires the prior authorisation from the information regulator, it MUST NOTIFY the information regulator thereof.

- Criminal offence: If the Company does not notify the information regulator, it is guilty of an offence, and is liable to a fine, or to imprisonment for a period not exceeding 12 months, or to both a fine, and imprisonment.

2.25.5. If the Company, as the responsible party, has notified the information regulator that it is processing information that requires the prior authorisation from the information regulator, it MUST STOP PROCESSING the information until the information regulator has completed its investigation, or until it receives a notice from the information regulator that a more detailed investigation will not be conducted, which notice MUST be provided in writing, within four (4) weeks of the notification, as to whether, or not, the information officer will conduct a more detailed investigation.

- Criminal offence: If the Company does not stop processing the information that requires the prior authorisation from the information regulator, it is guilty of an offence, and is liable to a fine, or to imprisonment for a period not exceeding 12 months, or to both a fine, and imprisonment.

2.25.6. If the information regulator decides to conduct a more detailed investigation, it MUST indicate the period within which it plans to conduct this investigation, which period MUST not exceed thirteen (13) weeks.

2.25.7. After the more detailed investigation, the information regulator MUST ISSUE a statement about the lawfulness of the information processing.

2.25.8. If the information processing is not lawful, the statement by the information regulator is deemed to be an enforcement notice.

- Criminal offence: If the Company does not comply with the enforcement notice, it is guilty of an offence, and is liable to a fine, or to imprisonment for a period not exceeding ten (10) years, or to both a fine, and imprisonment.

2.25.9. Where the Company has stopped processing information that requires the prior authorisation from the information regulator, while waiting for a decision by the information regulator, if it does not receive a decision from the information regulator within the four (4), and thirteen (13), weeks, respectively, it may presume that the information regulator has decided in its favour, and MAY RE-START PROCESSING the affected information.

2.25.10.

2.26. Disclosure of Personal Information

2.26.1. The Company may disclose a Data Subject's Personal Information to any of the Company's associates, relevant product suppliers and relevant third-party service providers. The Company has agreements in place, to ensure compliance with the confidentiality and privacy, conditions.

2.26.2. The Company may share a Data Subject's Personal Information with and obtain information about a Data Subject from, third parties, but only for the reasons specified in this Policy.

2.26.3. The Company may disclose a Data Subject's information where it has a duty or a right, to disclose the information in terms of applicable legislation, the law or where it may be deemed necessary, to protect the rights of the Company.

2.26.4. **Direct Marketing and Form 4:** Where the Company wishes to use personal information for direct marketing by means of unsolicited electronic communications (email, SMS, or automated calling), it will first obtain consent using Form 4, as prescribed under the POPIA Regulations. Data Subjects may withdraw consent at any time and may object to processing using Form 1.

2.27. Safeguarding Personal Information

2.27.1. Personal Information of Data Subjects must be adequately protected. The Company continuously reviews its security controls and processes, to ensure that Personal Information is secure.

2.27.2. The Company is a Responsible Party that is a juristic person and a private body. Therefore, the information officer must be the chief executive officer of the Company or a person duly authorised by the chief executive officer.

2.27.3. The chief executive officer has authorised **FC Greeff for Quantum Wealth Management** and **Stefan Greeff for Quantum Fund Managers** as the Information Officer, whose contact details are reflected elsewhere in this Policy and who is responsible for compliance with the conditions of the lawful processing of Personal Information and other provisions of the POPIA and the regulations thereto.

2.27.4. This Policy has been put in place throughout the Company and training about this Policy and the POPIA, will be provided to employees regularly.

2.27.5. Each new employee must sign an employment contract, containing relevant consent clauses for the use and storage of employee Personal Information or any other action required, in terms of the POPIA.

2.27.6. Current employees must sign an addendum to their employment contracts, containing relevant consent clauses for the use and storage of employee Personal Information or any other action required, in terms of the POPIA, if the relevant clauses are not included in the employment contracts.

2.27.7. Archived client Personal Information is stored **on AtWork**. Access to retrieve the archived Personal Information is restricted to individuals authorised by the Information Officer.

2.27.8. The agreements that the Company has in place with its responsible parties, product suppliers and third-party service providers, must stipulate that the responsible parties, product suppliers and third-party service providers, are responsible for complying with the POPIA and the regulations thereto.

2.27.9. Electronic files and data are backed up daily to internal systems, and monthly to an external hard drive, which is stored securely off-site. The process is verified manually and supported by an outsourced IT provider.

2.27.10. **The Information Officers** are responsible for the oversight of information security, in collaboration with management and the outsourced IT provider. Appropriate technical and organisational measures are in place to prevent unauthorised access and to ensure system resilience.

2.28. Access to and correction of, Personal Information

2.28.1. **Information officer contact details**

- **For Quantum Wealth Management:**
  Full name: FC Greeff

Email address: fc@quantumwealth.co.za

Telephone number/s: +27 12 346 0084

- **For Quantum Fund Managers:**

Full name: Stefan Greeff

Email address: stefan@quantumwealth.co.za

Telephone number/s: +27 12 346 0084

2.28.2. **Company's head office details**

Physical address:	Office Co, 2nd Floor, 90 Florence Ribeiro Ave, Nieuw Muckleneuk, Pretoria
Contact email address:	info@quantumwealth.co.za
Contact telephone number/s:	+27 12 346 0084

3. Direct marketing

3.1. The Company MUST NOT process the personal information of a data subject for the purpose of direct marketing through any form of electronic communication, including automatic calling machines (that is a machine that can make automated calls without human intervention), facsimile machines, SMSs, or e-mail, UNLESS the data subject:

- has given their consent to the processing of their personal information; or
- is a client of the responsible party, subject to specified conditions.

3.2. If the data subject's consent is required, BEFORE the Company is permitted to approach the data subject through direct marketing, AND where the data subject has not previously withheld their consent, it may approach the data subject ONLY ONCE, to obtain their consent, using FORM 4.

3.3. Where the data subject is a client of the Company, as the responsible party, IT MAY ONLY process the personal information through direct marketing:

- IF it has obtained the contact details of the data subject, in the context of the sale of a product, or service
- for the purpose of direct marketing its own similar products, or services; AND
- IF the data subject has been given a reasonable opportunity to object, free of charge, and in a way free of unnecessary formality, to this use of their electronic details:
- at the time when the information was collected; AND
- at the time of each communication with the data subject, for the purpose of marketing, IF the data subject has not initially refused this use.

3.4. The Company MUST ENSURE that ALL communication that is for the purpose of direct marketing CONTAINS:

- details of the identity of the sender, or the person on whose behalf the communication has been sent; AND
- an address, or other contact details, to which the recipient may send a request to stop the communications.

4. Directories

4.1. If the Company wants to include the personal information of a data subject in a printed, or electronic, directory of subscribers, which is available to the public, or obtainable through directory enquiry services, IT MUST INFORM the data subject, free of charge, and BEFORE the information is included in the directory:

- about the purpose of the directory; AND
- about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.
- This DOES NOT APPLY to editions of directories that were produced in printed, or off-line electronic, form BEFORE the commencement of this requirement.

4.2. The Company MUST GIVE a data subject a reasonable opportunity to object, free of charge, and in a way that is free of unnecessary formality, to this use of their personal information, or to request verification, confirmation, or withdrawal, of the information, IF

the data subject has not initially refused the use of their personal information for this purpose.

- This DOES NOT APPLY to editions of directories that were produced in printed, or off-line electronic, form BEFORE the commencement of this requirement.

4.3. If the Company has included the personal information of data subjects, who are subscribers to fixed, or mobile, public voice telephone services, in a public subscriber directory, in conformity with the conditions for the lawful processing of personal information, BEFORE the commencement of this requirement, the personal information of the subscribers MAY REMAIN included in the public directory, in its printed, or electronic, versions, AFTER having received the information required.

5. Automated decision making

5.1. The Company MUST ENSURE that IT DOES NOT subject a data subject to a decision that results in legal consequences for them, or which affects them substantially, which is based solely on the automated processing of personal information, intended to provide a profile of the person, including their performance at work, or their credit worthiness, reliability, location, health, personal preferences, or conduct.

5.2. These provisions DO NOT APPLY IF the decision:

- has been taken in connection with the conclusion, or execution, of a contract, AND:
- the request of the data subject, in terms of the contract, has been met; OR
- appropriate measures have been taken to protect the data subject's legitimate interests; OR
- is governed by a law, or code of conduct, in which appropriate measures are specified for protecting the legitimate interests of data subjects.
- The appropriate measures, in terms of the law, or code of conduct, MUST:
  - provide an opportunity for a data subject to make representations about a decision; AND

- require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information about them, to enable them to make representations about the decision.

5.3. Transfers of personal information outside South Africa

5.3.1. The Company, as a responsible party in South Africa, MUST ENSURE THAT IT DOES NOT TRANSFER personal information about a data subject to a third party, who is in a foreign country, UNLESS:

- the third party, who is the recipient of the information, is subject to a law, binding corporate rules, or binding agreement, which provide an adequate level of protection that:
- effectively upholds principles for reasonable processing of the information that are substantially like the conditions for the lawful processing of personal information about a data subject, who is a natural person, and, where applicable, a juristic person; AND
- includes provisions that are substantially like these requirements, relating to the further transfer of personal information from the recipient to third parties, who are in a foreign country
- the data subject consents to the transfer
- the transfer is necessary for the performance of a contract between the data subject and the Company, or for the implementation of pre-contractual measures taken in response to the data subject's request
- the transfer is necessary for the conclusion, or performance, of a contract, concluded in the interest of the data subject, between the Company, and a third party; OR
- the transfer is for the benefit of the data subject, AND:
- it is not reasonably practicable to obtain the consent of the data subject to that transfer; AND
- if it were reasonably practicable to obtain the consent, the data subject would be likely to give it.

6. Complaints

6.1. The Company should inform people that they may submit a complaint to the information regulator, by using Part I of FORM 5, alleging interference with the protection of the personal information of a data subject.

6.2. The Company, as a responsible party, MAY submit a complaint to the information regulator, by using Part II of FORM 5, if it is aggrieved by the determination of an adjudicator.

6.3. The Company should inform data subjects that they MAY submit complaints to the information regulator, by using Part II of FORM 5, if they aggrieved by the determination of an adjudicator.

7. Offences and penalties

7.1. The Company MUST ENSURE that it complies with enforcement notices issued to it by the information regulator, because it is guilty of an offence if it does not comply.

7.2. The Company MUST ENSURE that it does not knowingly make false statements, or recklessly make materially false statements, in response to information notices, because it is guilty of an offence to do so.

7.3. The Company MUST ENSURE that it DOES NOT contravene the provisions of conditions for lawful processing, insofar as those provisions relate to the processing of an account number of a data subject (unique identifier, providing access to own funds, or credit facilities), because it is guilty of an offence to do so.

8. Consequences of non-compliance with the policy

8.1. All employees are obliged to comply with the Policy and it is a condition of employment. Non-compliance is a breach of their employment contract and is an action of misconduct, so employees may be subject to disciplinary action, which may lead to dismissal. Non-compliance by an employee will be dealt with according to the Company's disciplinary policy. For assessing and addressing, the non-compliance, reports made by the Compliance Officers, internal audit, external audit and the Authorities, will be considered, for appropriate action to be taken.

9. Policy review

9.1. The policy will be reviewed annually, updated if necessary, and the latest version will be adopted and approved, by the board.

10. Data breach register

The Company will maintain a register of all personal data breaches, regardless of whether they are notifiable to the Information Regulator. Please see a template register in Annexure A. The Company retains all breach records in the breach register for a minimum of 5 years from the date of the incident, whether or not the breach was notifiable.

11. Response plan

According to the Company's response plan the Information Officer will:

- Make an urgent preliminary assessment of what data has been lost, why and how.
- Take immediate steps to contain the breach and recover any lost data.
- Undertake a full and detailed assessment of the breach.
- Record the breach in the Company's data breach register.
- Notify the Information Regulator where the breach is likely to result in a risk to the rights and freedoms of Data Subjects.
- Notify affected Data Subjects where the breach is likely to result in a high risk to their rights and freedoms.
- Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Please see Annexure B for more information

Annexure A: Data Breach Register

QWM & QFM Data Breach Register

Date the breach occurred	Description of the breach	Breach category Confidentiality Availability Integrity	Breach Reported to IR Yes No N/A	Number of Data Subjects affected	Data Subject impact classification Serious Moderate None	Number of records affected	Reported to Data Subject Yes No N/A	Impact of the breach on FSP Name	Remedial action taken

Annexure B: Data Breach Response plan for FSP Name

CONTAIN

- Data breaches must immediately on discovery be reported to the Information Officer who will drive implementation of this plan.
- If the breach took place through an electronic device:
  - Take the device offline immediately, but DO NOT shut it down
  - Change passwords

ASSESS

- Determine the extent of the breach
  - who was affected
  - which records have been affected
- Determine the impact of the breach
- Determine if the breach should be reported to
  - the Information Regulator
  - Data Subjects

MANAGE

- Agree what the appropriate actions will be
  - Facilitate technology restoration or recovery if applicable
  - Prepare and submit insurance claim
- Communicate decisions internally
- Prepare (and arrange for authorisation of) and Communicate with Customer(s) / Public
- Take remedial action to prevent similar breaches

APPENDIX D PRODUCT AND SERVICE SUPPLIERS

1. ABSA Life Ltd.
2. Allan Gray Life Ltd.
3. Allan Gray Unit Trust Management (RF) (Pty) Ltd.
4. Ashburton Fund Managers (Pty) Ltd.
5. Boutique Collective Investments (RF) (Pty) Ltd.
6. Boutique Investment Partners (Pty) Ltd.
7. Brightrock (Pty) Ltd.
8. Discovery Life Ltd.
9. FMI a division of Bidvest Life Ltd.
10. Glacier International
11. Hollard Life Assurance Company Ltd.
12. Investec Bank Ltd.
13. Liberty Group Ltd.
14. MMI Group Ltd.
15. Momentum Collective Investments (RF) (Pty) Ltd.
16. Ninety One SA (Pty) Ltd.
17. Old Mutual Life Assurance Company (South Africa) Ltd.
18. Old Mutual Unit Trust Managers (RF) (Pty) Ltd.
19. Professional Provident Society Insurance Company Ltd.
20. Professional Provident Society Investment Proprietary Ltd.
21. Prudential Investment Managers (Pty) Ltd.
22. Sanlam Life Insurance Ltd.
23. **Shares**
24. Momentum Wealth (Pty) Ltd.
25. Sanlam Private Wealth (Pty) Ltd.
26. PSG Online (Pty) Ltd.