PAIA & POPIA MANUAL

1. INTRODUCTION

The Promotion of Access to Information Act, 2 of 2000 ("PAIA") gives effect to section 32 of the Constitution, that provides for access to information if a person wants to exercise a right or to protect a right, subject to the procedural requirements laid down by PAIA. For this purpose, PAIA requires that the FSP must implemented a manual in terms of Section 51 of PAIA setting out the procedures to be followed to have access to Information which procedures are set out in this Manual.

The Protection of Personal Information Act, 4 of 2013 ("POPIA") on the other hand provides for 8 protection principles that FSP's must comply with to protect the Personal Information of all Data Subjects. The FSP must implement a Manual that must comply with section 14 and 51 of PAIA and is required to make it available to persons who want to access FSP's Personal Information. Should a person having a right to the Personal Information, require access to these Personal Information, then access is allowed by following the procedures laid down by PAIA and as set out in this Manual.

2. PURPOSE

The purpose of the Manual is to:

- provide details on records and information of the FSP that are available and accessible once the requirements for access have been met; and
- sets out the procedures to be followed by a person that wants access to information, (including POPIA Personal Information) that are subject to protection and non-disclosure, if such person wants to exercise or to protect a right; and
- provide a guide on POPIA legislation how FSP process Personal Information.

3. AVAILABILITY OF THE MANUAL

The Manual is made available in terms of Section 4 of the Regulations to POPIA:

- on the FSP's website www.navigatefm.co.za
- by contacting the Information Officer at the contact details provided below. A fee will be levied if copies of the Manual is required and as provided for in terms of Appendix 3.
- at the offices of FSP for inspection during normal business hours at no cost.

4. INTRODUCTION TO THE COMPANY AND TYPE OF BUSINESS

- Name: Navigate Financial Advisors (Pty) Ltd
- FSP No. 46393
- **Type of business:** FSP does not form part of a group of companies and is authorised Category I Financial Services Provider ("FSP") with the Financial Sector Conduct Authority ("FSCA") with FSP no. 46393 in terms of the Financial Advisory & Intermediary Services Act 37 of 2002 ("FAIS") and provides financial services (advise and intermediary services) to Clients by focusing mainly on retirement savings.

5. COMPANY CONTACT DETAILS (PAIA Section 51(1)(a))

Designated and authorised persons:

- **Director:** Neil Tillemans

Contact details:

- **Postal address:** 23 Main Street, Newlands, 7700
- **Business address:** 23 Main Street, Newlands, 7700
- **Telephone Number:** 021 447 1049
- **Website:** www.navigatefm.co.za

Information and Deputy Information Officers:

- **Information Officer:** Neil Tillemans and email address: neil@navigatefm.co.za

6. THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION ("SAHRC") GUIDE ("PAIA GUIDE") (PAIA Section 51(1)(b))

- PAIA 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.
- Requests in terms of PAIA shall be made in accordance with the prescribed procedures and at the rates provided for in in terms of the PAIA Regulations.
- Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission. It contains information on how to use and apply PAIA for the purposes of exercising Constitutional Rights.
- The PAIA Guide is available in all 11 official languages and can be obtained by contacting the FSP or the Information Regulator (South Africa). It can also be downloaded from the Information Regulator (South Africa) website.
- Contact details for the Information Regulator (South Africa):
  - **Address:** JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
  - **P O Box:** 31533, Braamfontein, Johannesburg, 2017
  - **E-mail:** inforeg@justice.gov.za
  - **Website:** https://www.justice.gov.za/inforeg/docs.html

7. PUBLICATION AND AVAILABILITY OF INFORMATION AND RECORDS

7.1 Applicable Legislation:

The legislation applicable to FSP are contained in **Appendix 1** of this Manual. FSP may be required to obtain information and keep records in terms of these legislation and depending on the relevant legislation requirements, FSP may also be required to make certain information or Records publicly available, allow disclosure of information or Records subject to certain conditions or may be prevented to disclose information or Records**.** The Requester's right of access to information or a Record must be dealt with taking into consideration the applicable legislation requirements.

7.2 Available Records **(**PAIA Section 51(1)(d)**)**

Examples of record Categories and available Records that are applicable to the FSP are contained in **Appendix 2** of this Manual. The inclusion of a category or examples of Records does not mean that the Information and Records falling withing those categories will automatically be made available to a Requester.

Records may be available as follows:

- Freely if publicly available e.g. information and records available on the FSP's public website;
- Made available but subject to Copyright;
- Made available but subject to limited disclosure.

Note that a person may only request information from **the FSP** as a Private Body if the requested information is required for the exercise or protection of a right. Certain grounds of refusal may also apply as indicated below in paragraph 8.4 to a request for such record.

8. FORM OF REQUEST TO ACCESS INFORMATION AND RECORDS (PAIA Section 51(1)(e))

8.1 Requester

- Personal Requester: A Personal Requester is a requester who is seeking access to a record containing Personal Information about the Requester itself. Access will be granted by the FSP subject to applicable legislation.

- Other Requester: If a person other than the Personal Requester is seeking access to a record containing Personal Information, then the FSP is not obliged to grant access to such record, unless such person fulfils the requirements for access as provided for in terms of PAIA.

8.2 Request for Access to Record Procedures

The procedures to follow are as follows:

- A Requester must complete and sign the prescribed form enclosed herewith in **Appendix 3** together with payment of the required fee (only if it is an Other Requester).
- The completed and signed form together with proof of payment must either be posted, submitted per hand or be emailed to the Information Officer at the email address stated above.
- If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the Information Officer.
- If a request is made on behalf of another person, the Requester must then submit proof of the capacity in which the Requester is making the request on behalf of the other person to the satisfaction of the Information Officer.
- All required information must be provided on the **Appendix 3** form and the information must be true complete and correct with enough particularity to enable the Information Officer to identify:
  - the Requester's identity;
  - contact details of the Requester;
  - the requested record/s, and
  - the form of access required by the Requester.
- A Requester may only request access to a record in order to exercise or protect a right and must clearly state what the nature of the right is so to be exercised or protected. The requester is further required to provide an explanation of why the requested record is required for the exercise or protection of that right.
- The FSP will process a request to access a record within 30 (thirty) days of receipt of the completed **Appendix 3** form together with proof of payment, if applicable, unless the Requestor has stated exceptional reasons and circumstances together with proof, if applicable, that would satisfy the Information Officer that the time period not be complied with.
- The FSP shall inform the Requester in writing whether access has been granted or denied together with reasons thereof.
- If the Requester requires access to the records in another manner, the Requester must state the manner and the particulars so required.

8.3 Fees Payable

The applicable fees that are prescribed in terms of the PAIA Regulations are as follows:

- A non-refundable prescribed request fee is payable up on submission of any request for access to any record before a request will be processed.
- The fees above do not apply if the request is for personal records of the person requesting **–** in this instance no fee is payable.
- If the preparation of the record requested requires more than the prescribed hours (currently 6 hours), a deposit shall be paid (of not more than one third of the access fee which would be payable if the request were granted).
- A requestor may lodge an application with a court against the tender/payment of the request fee and/or deposit.
- Records may be withheld until the fees have been paid by the Requester.
- Fees are subject to confirmation by the Regulator in the Government Gazette and any applicable fees or changes will be upfront disclosed to Requesters.
- A List of the current Fees payable are set out in **Appendix 4**.

8.4 Grounds for refusal of a Request

Chapter 4 of PAIA provides for several grounds on which a request for access to Personal Information must be refused. These grounds may include where:

- the privacy and interests of other individuals are protected, including a deceased person, where disclosure would be unreasonable;
- such records are already otherwise publicly available;
- the public interests are not served;

- the mandatory protection of commercial information of a third party/ company which include trade secrets, financial, commercial or technical information that may cause harm if disclosed and information that could put a third party/ Company in disadvantage in contractual/ other negotiations or commercial competition or computer programs owned by a company protected by copyright and intellectual property laws;
- the mandatory protection of certain confidential information of a third party;
- the mandatory protection of confidential information of third parties if it is protected in terms of an agreement;
- mandatory protection of the safety of individuals and protection of property;
- mandatory protection of Records that are privileged in legal proceedings
- research information of a third party/ Company if disclosure would put the research or researcher in disadvantage.
- Requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

8.5 Information or Records not found

If information or Records cannot be found despite reasonable and diligent searches by the FSP, then the Information Officer must provide the Requester with a notice in the form of an affidavit setting out the measures taken to locate the document and the inability to locate it.

8.6 Remedies available to a Requester if access is refused

The decision made by the Information Officer is final and Requesters must exercise external remedies if the Request for access to Information or Records is refused. A Requester may however apply to a court for relief within 180 days of notification of the decision for appropriate relief as provided for in terms of sections 56(3) (c) and 78 of PAIA.

9. POPIA REQUIREMENTS WHEN PROCESSING PERSONAL INFORMATION

The FSP applies the following protection principles as provided for in terms of POPIA when processing Personal Information. Specific details on how the FSP is processing Personal information is also set out in **Appendix 5** of this Manual.

9.1 THE RESPONSIBLE PARTY'S RESPONSIBILITIES:

9.1.1 Accountability:

This principle contemplates the assigning of responsibility by the Responsible Party to oversee and ensure compliance with the POPIA requirements by means of:

- Appointment of an Information Officer and a Deputy Information Officer who must register with the Information Regulator.
- Audit the processes used to collect, record, store, disseminate and destroy Personal Information.
- Ensure the integrity and safekeeping of Personal Information in possession or under control.
- Take steps to prevent the information being lost or damaged, or unlawfully processed or accessed.
- Ensure staff is properly trained on a regular basis to understand their responsibilities and consequences of non-compliance with POPIA.

9.1.2 Processing Limitation:

Personal Information may only be processed by the Responsible Party if it is done lawfully in a manner that does not infringe the privacy of the Data Subject. Processing must be adequate, relevant and not excessive given the purpose and if consent was obtained from the Data Subject, then such consent must be voluntary and specific.

9.1.3 Purpose Specification:

Purpose Specification is important to determine the scope within which Personal Information may be processed by a Responsible Party. The Responsible Party is required to define the purpose of collecting the Personal Information clearly, indicate it is collected for a specific, explicitly defined and lawful purpose; collect only the necessary information and be clear to whom the information is transferred, ensure that Personal information is destroyed, deleted or 'de-identified' as soon as the purpose for collecting the information has been achieved, subject to other legislation e.g. FAIS and FICA (5-year record keeping requirements), and indicate that further restrictions apply on the transfer of Personal Information out of South Africa and to transfer Personal Information back into South Africa. (Restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned).

9.1.4 Further Processing limitation:

Once the Responsible Party has identified and obtained consent for specific, legitimate and explicitly defined purposes, then Personal Information cannot be processed contrary to the purpose for which it was collected. The processing of such Personal Information may only occur insofar as it is necessary for the fulfilment of the purpose. If information is received via a third party for further processing, then this further processing must be compatible with the purpose for which the data was initially collected, otherwise further consent must be obtained.

9.1.5 Information quality:

The Responsible Party must ensure and maintain the quality of the Personal Information that it processes. It must therefore:

- take reasonably practicable steps to ensure that the Personal Information is complete, accurate and updated
- consider obtaining a warranty from Data Subjects to ensure that the Personal Information is correct and updated.

9.1.6 Openness required:

The Responsible Party is required to notify the Information Regulator of the applicable data subject groups that the information is used for e.g. financial services category. The Responsible Party has a duty to process Personal Information in a fair and transparent manner and must take steps to notify the Data Subject whose Personal information is being processed that this is being done together with reasons. The Data Subject must be informed about the purpose and from what source his Personal Information was obtained:

- the name and address of the company processing the Personal Information
- whether the provisioning of the Personal Information is voluntary or mandatory

9.1.7 Security safeguards:

Personal Information should be kept secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure. The Responsible Party is required to secure the integrity of personal information by taking appropriate, reasonable technical and organisational measures to prevent loss, damage, unauthorised access and unlawful access or processing of Personal Information.

<u>The FSP as Responsible Party must take all reasonable measures to:</u>

- Identify all reasonably foreseeable internal and external risks
- Establish and maintain appropriate safeguards against the risks
- Regularly verify that the safeguards are adequately implemented
- Ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

<u>The FSP as Responsible Party must oversee an Operator who processes data on his/her behalf and ensure that the Operator:</u>

- Treat information confidentially
- establishes and maintains appropriate security safeguards
- ALL processing by an operator is governed by a written contract
- In the event of security breaches, the Responsible Party must notify the Regulator and also the Data Subject (if required).

9.1.8 Participation:

POPIA allows for Data Subjects to make certain requests, free of charge, to organisations that holds their Personal Information. Data Subjects may request access to or records of their Personal Information and/or request the correction or deletion of any Personal Information held by it. Data Subjects may also request that inaccurate, misleading or outdated Personal Information be updated and has the right to know the identity of all third parties that have had access to their information.

9.2 EXCLUSIONS

POPIA protection does not apply to the following information:

- **The processing of Personal Information:**
  - in the course of a purely personal or household activity;
  - that has been de-identified to the extent that it cannot be re-identified again;

- by or on behalf of a public body —
  - which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defense or public safety; or
  - the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;
- by the Cabinet and its committees or the Executive Council of a province; or
- relating to the judicial functions of a court referred to in section 166 of the Constitution of the Republic of South Africa, 1996.

- **''Terrorist and related activities''** for purposes of subsection (1)(c), means those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).
- Data Subject consent is not required, in instances where it would **prejudice a lawful purpose or the information is publicly available.**

9.3 OPERATOR'S RESPONSIBILITIES INCLUDE:

All Information processed by an operator must be treated in the following manner:

- The Responsible party must be aware of the Operators processing.
- The Operator must treat information confidentially.
- The Responsible party must ensure that the Operator establishes and maintains appropriate security safeguards.
- In the event of security breaches, the Operator via the Responsible party must notify the Regulator and the data subject.
- The processing by an operator must be governed by a written contract between the Responsible party and the Operator.

The contents of the contract between the Operator and the Responsible Party must detail at least the following:

- the legitimate grounds for collecting and using personal data collected,
- the lawful purpose for which data are being collected,
- the limit of processing and prohibiting of further processing,
- the extent of information that is required to prevent any excessive information collection,
- the information retention periods and requirements applicable together with destruction processes and procedures,
- The right of individuals to request such information and query the use thereof,
- The security measures required to prevent the unauthorised or unlawful processing of personal data or access to personal data, including accidental loss or destruction or damage to personal data.

9.4 DEALING WITH SPECIAL PERSONAL INFORMATION

If an objection is received from a Data Subject to process Special Information, then this information may not be supplied to 3rd parties without the Data Subject's consent.

- **Religious or Philosophical Beliefs processing:** May take place by Spiritual or religious organisations & institutions, provided that the information concerns data subjects belonging to such organisations; if it is necessary to achieve their aims and principles; or to protect the spiritual welfare of the data subjects.

- **Race processing** may be carried out to Identify data subjects when this is essential and to Comply with laws or measures designed to protect or advance persons disadvantaged by unfair discrimination.

- **Trade Union Membership processing** may take place by a trade union to which the data subject belongs, or the trade union federation to which the trade union belongs, if the processing is necessary to achieve the aims of the trade union/trade union federation.

- **Political Persuasion processing** may take place by an institution founded on political principles if such processing is necessary to achieve the aims or principles of the institution.

- **Health or Sexual Life processing** must be confidential and may take place by:
  - Medical practitioners, healthcare institutions
  - Insurance companies, medical aid scheme providers

- Schools
- Institutions of probation, child protection or guardianship
- Pension funds and employers if processing is necessary for:
  - Implementation of laws/pension regulations
  - Re-integration/support for workers or persons entitled to benefit in connection with sickness/work incapacity

- **Criminal behaviour processing** may take place by:
  - Bodies charged by law with applying criminal law
  - Responsible parties who have obtained the information in accordance with the law
  - Responsible parties who process the information for their own lawful purposes to; to assess an application by a data subject in order to take a decision about or provide a service to that data subject to protect their legitimate interests in relation to criminal offences.

- **General Exemptions**
  The Regulator may authorise processing of any information, which will not be in breach of POPIA, if the public interest includes:
  - the legitimate interests of State security
  - the prevention, detection and prosecution of offences
  - important economic and financial interests of the State or a public body
  - historical, statistical or research activity.

9.5 DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATIONS

Direct marketing is prohibited unless you have consent, or the target is already a customer. You may only approach a person for consent once and if they have not previously withheld such consent and may only use the information for the initial purpose why it was obtained for. Any communication for the purpose of direct marketing must contain Details of the identity of the sender, and the address or other contact details to which the recipient may send a request to opt-out.

9.6 OBJECTION TO PROCESS PERSONAL INFORMATION

A person that wants to object to the processing of Personal Information in terms of section 11(1)(d) to (f) of POPIA, must complete, sign and submit to the Information Officer the Form contained **Appendix 6** of this Manual. Affidavits or other documentary proof may be submitted with the Form in support of the objection.

- **REQUEST FOR A) CORRECTION OR DELETION OF PERSONAL INFORMATION; OR FOR B) DESTRUCTION OR DELETION OF PERSONAL INFORMATION IN POSSESSION OF UNAUTHORISED PERSON**
  Person that wants to submit a request to rectify, delete or destroy Personal Information in terms of section 24 of POPIA, must complete, sign and submit to the Information Officer the Form contained in **Appendix 7** of this Manual. Affidavits or other documentary proof may be submitted with the Form in support of the request.

9.7 COMPLAINTS IN TERMS OF POPIA

- A Person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the Personal Information of a Data Subject.
- A Responsible Party or Data subject may, in terms of section 63(3), further submit a complaint to the Regulator in the prescribed manner and form if he/ she/ it is aggrieved by the determination of an adjudicator.
- The contact details of the Information Regulator are as follows:
  - **Business address:** JD House, 27 Stiemens street, Braamfontein, Johannesburg, 2001
  - **Postal address:** P O Box 31533, Braamfontein, Johannesburg, 2017
  - **E-mail:** complaints.IR@justice.gov.za
  - **Website:** www.justice.gov.za