Finfocus POPIA Policy (2023)

In terms of the Protection of Personal Information Act 4 of 2013 ("POPIA"), Finfocus Financial Planners (Pty) Ltd undertakes to hold the personal information in our possession in accordance with the principles outlined in POPIA. This document forms part of the organisation's regulatory Risk Management & Compliance Management procedures that are in place. The document sets out the processes and procedures intended to guarantee that Finfocus's compliance obligations are in place at all times and that non-compliance is avoided.

POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to the "organisation" includes the "policy owner".
- Finfocus's governing body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to know the policy's requirements and to comply with the stated processes and procedures.
- The MD & deputy information officer are responsible for overseeing and maintaining control procedures and activities.

TABLE OF CONTENTS

1. INTRODUCTION

The right to privacy is protected in the South African Constitution in the Protection of Personal Information Act 4 of 2013 (POPIA).

Principles to protect personal information will be applied to process personal information in a context-sensitive manner. Without access to the personal information of clients a financial planning services provider is not able to work. Safe-guarding all information regarding a client is therefore part of the ongoing process to provide a client with holistic personal financial planning. This is part of establishing and maintaining a long-term relationship of trust and mutual respect with a client.

The following ongoing processes are in place:

(i) There is no engagement with a client without a signed consent form with regard to POPIA; this is uploaded on the company's CRM (client relationship management) system

(ii) The MD is the Information Officer. Both he and the deputy information officer have been appointed; the information of both individuals has been uploaded on the POPI registration data base

(iii) The company's clients have been evaluated and have been assessed with regard to personal risk with regard to their personal financial situation and ML & TF risks (see the procedures in place to determine risk regarding both clients and products)

(iv) No product is issued to a client without signed POPI consent & source of funds indications

(v) Since all clients sign POPI forms on an on-going basis, periodic spot-checks are sufficient

(vi) POPI procedures form part of the CRM system and, just as FICA regulatory requirements, are in place for each client

2. DEFINITIONS

2.1. Personal information

This is any information identifying a client. It is connected to an identifiable living human being. It includes information relating (but not limited) to

(a) race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person;
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

2.2 Data subject

This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the organisation with products or other goods.

2.3 Responsible party

The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case Finfocus is the responsible party.

2.4 Operator

An operator is 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. For example, a third-party service provider that has contracted with the organisation to shred documents containing personal information.

2.5 Information officer

The information officer is responsible for ensuring the organisation's compliance with POPIA. The information and deputy information officer have been registered with the South African Information Regulator (established under POPIA). The MD of Finfocus, Schalk van Niekerk, CFP® is the information officer and Dr. Sjarlene Thom, CFP®, is the deputy information officer.

2.6 Processing

The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

- 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; or
- merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 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 so 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 or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 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.

2.9 Unique identifier

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

2.10 De-identify

This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies that data subject.

2.11 Re-identify

In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

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

2.13 Direct marketing

Means to approach a data subject, either in person or by electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods and services to the data subject or requesting the data subject to make a donation of any kind for any reason.

2.14 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.

3. POLICY PURPOSE

This purpose of this policy is to protect the organisation from the compliance risks associated with the protection of personal information which includes:

- breaches of confidentiality. For instance, the organisation could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately;
- all data subjects should be free to choose how and for what purpose the organisation uses information relating to them. Let is be noted that Finfocus clients sign a POPI consent form which indicates very clearly that the client's personal information is required in order to conduct the business of financial planning for the client. Choosing not to supply this information means that no business can be conducted with such a client. Offering a choice not to make personal information available where needed is therefore not an option for a financial planning company.
- reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the organisation.

This policy demonstrates the organisation's commitment to protecting the privacy rights of data subjects in the following manner:

- through stating desired behaviour and directing compliance with the provisions of POPIA and best practice;
- by cultivating an organisational culture that recognises privacy as a valuable human right;
- by implementing internal best practice procedures to ensure the compliance risk associated with the protection of personal information is minimal;

- 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 organisation;
- by assigning specific duties and responsibilities the Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the organisation and data subjects.

Finfocus staff know that both FICA and POPIA requirements are implemented on an ongoing basis. This is nothing new. Awareness have been ingrained by training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. Policy application

The policy as well as its principles applies to the whole of Finfocus, including all employees, volunteers, contractors, suppliers and other persons acting on behalf of Finfocus.

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

POPIA compliance is activated in any situation where there is:

- A **processing** of……..
- ……**personal information**…….
- ……..entered into a **record**…….
- ……..by or for a **responsible person**……

  ……..who is **domiciled** in South Africa

POPIA does not apply in situation where the processing of personal information

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified

5. Rights of data subjects

Finfocus will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects, at the same time making clear the need to access personal information in order to do business as a financial planning company.

Finfocus will ensure that it gives effect to the following six rights

5.1 <u>The right to access personal information</u>

Finfocus recognises that a data subject has the right to know whether Finfocus holds personal information related to him/her/it, including the right to access that personal information. See Annexure A for a 'Personal information request form'.

5.2 <u>The right to have personal information corrected or deleted</u>

The data subject has the right to request where necessary, that his/her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information. Since FICA regulations require a financial planning firm to keep all records regarding a client relationship for 5 years after the relationship has come to an end, this right can only be exercised after this period.

5.3 <u>The right to object to the processing of personal</u> <u>information</u>

The data subject has the right to object, but if Finfocus needs the information in order to do business with the client, the client will either agree to processing of personal information or the

relationship will cease. Finfocus has forwarded an explanatory letter to each client regarding the need to sign a POPI consent form. This letter explains why Finfocus needs access to a data subect's personal information as requested in the so-called "POPI form" required to be signed by clients. See an example in Annexure A of both the POPI form required to be signed and the explanatory letter with regard to the need of signing the form.

5.4 The right to object to direct marketing
The client's right to object to unsolicited electronic communications is self-evident.

5.5 The right to complain to the information regulator
The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

An example of a "POPI Complaint Form" can be found under Annexure B.

5.6 The right to be informed
The data subject has the right to be notified that his, her or its personal information is being collected by the organisation's request that the data subject sign the POPI form. The data subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. General guiding principles
All employees and persons acting on behalf of the organisation will at all times be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability
The protection of personal information is everybody's responsibility. Finfocus will ensure that the POPIA provisions are complied with. Finfocus will take disciplinary action against anyone who through intent or negligence and/or omissions fail to comply with the principles outlined in this policy.

6.2 Processing limitation
Personal information under Finfocus's control will be processed

- in a fair, lawful and non-excessive manner
- only with the informed consent of the data subject, and
- only for a specifically defined purpose

Finfocus will inform the data subject why the collection of personal information is needed and obtain written consent to process this information. Where services are concluded electronically, the data subject's consent will also be obtained. Finfocus will not share personal information with any company or individual not directly involved with the purpose for which the information was originally collected. The data subject will be informed that personal information is shared as part of the ongoing financial planning process without which the financial planning service is not possible.

6.3 Purpose specification
All operations are informed by the principle of transparency. Personal information is processed only for specific, defined & legitimate reasons. The data subject is informed of these reasons in the explanatory letter sent out to all Finfocus clients.

6.4 Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. If personal information is held for another purpose than that for which it was originally collected and if this secondary purposed is not compatible with the original purpose the data subject's consent will be obtained.

6.5 Information quality

Finfocus will ensure that personal information collected is complete, accurate and not misleading. For instance the beneficiary details of a life insurance policy are of the utmost importance and Finfocus will put great effort into ensuring its accuracy. If personal information is obtained from third parties, Finfocus will take reasonable steps to confirm that the information is correct by verifying the information directly with the data subject.

6.6 Open communication

Finfocus does not collect personal information from data subjects without informing the data subject and asking for written consent. Any client will know the different contact numbers or individuals to contact when a client wants to be informed regarding the personal information kept by Finfocus. No personal information is collected without a data subject's written consent, therefore the data subject will at all times know that the company indeed holds its personal information (without which a financial planning relationship cannot exist). The data subject will therefore be able, at any time, to

- request access to the personal information supplied to Finfocus by the data subject itself;
- request any updates (with proof that the update information is correct, for instance stamped bank statement for a new bank account number);
- make a complaint regarding the processing of the information;
- a complaint that the information is required cannot be entertained, since without the consent to collect the information, no relationship with Finfocus is feasible

6.7 Security safeguards

Please see attached (at the end of this document) the Certificate of compliance of the product provider which provides Finfocus with the Client Relationship Management system on which all personal information of data subjects are held. Finfocus's IT supplier & marketing provider are similarly POPIA compliant. The third-party service providers' agreements regarding POPIA are also in place.

All security safeguards required are therefore in place.

All existing and new employees sign employment contracts containing confidentiality agreements. This is a requirement for any employee working with a client's confidential financial & personal information (regardless of the level of confidentiality required) irrespective of the more recent POPIA requirements.

Finfocus's confidentiality agreement with employees have long been included in any employee contract. The contract has recently been updated to keep pace with regulatory and other requirements regarding employment. Service level agreements regarding confidentiality are also in place.

6.8 Data subject participation

Data subjects may at any time update their information, provided proof of the new information is also supplied. Deletion of personal information is not always possible, even if the client terminates his/her relationship with Finfocus. Finfocus is required by law to keep all records of a data subject for 5 years after the termination of a client-service provider relationship.

Electronic newsletters can only be received on selecting to receive this information. These newsletters are not available if a choice to receive the letter has not been indicated.

7. Information officers

Finfocus has appointed an Information officer and a deputy information officer. The latter is responsible to ensure compliance with POPIA. The deputy information is appointed on a biennial basis. See the Information officer appointment letter in Annexure F.

8. Specific duties and responsibilities

8.1 Governing body

The accountability for POPIA cannot be delegated, but the duties may be delegated.
The governing body must ensure that:

- the information officer is appointed (even though Finfocus is not legally required to have one)
- all persons processing personal information are trained & supervised to do so
- understand that they are contractually obligated to protect the personal information they come into contact with
- are aware that wilful or negligent breach of this policy may lead to disciplinary steps taken against them
- data subjects who want to make enquiries about their personal information are made aware of their right to do so and how they should proceed
- a POPI audit is periodically scheduled to oversee the whole process with regard to personal information (how to collect, hold, use, share, disclose, destroy, etc. personal information)

8.2 Information officer

The information officer (deputy information officer) is responsible for:

- taking steps to ensure compliance with POPIA
- keeping the governing body updated about Finfocus's POPIA responsibilities; for instance in case of a security breach, the governing body must be informed
- keep up to date with privacy regulations and aligning them with Finfocus's personal information processing procedures, including reviewing the relevant policies
- oversee or conduct POPI audits regularly
- encourage data subjects (for instance checking at annual reviews whether all personal information is up to date) to update their personal information
- check any contracts with operators, employees, third parties who may have contact with data subjects personal information
- oversee compliance with processing of personal information
- ensure that employees are aware of the risks associated with the processing of personal information and remain aware of security controls
- oversee training of individuals involved in processing of personal information
- addressing employees' POPIA related questions
- working with the regulator regarding ongoing investigations; the information officer is the point of contact for the information regulator on issues relating to the processing of personal information

8.3 IT manager

See the service agreement with the external IT supplier who is responsible for:

- ensuring that the organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards
- ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services
- ensuring that servers containing personal information are sited in a secure location, away from the general office space
- ensuring that all electronically stored personal information is backed-up and tested on a regular basis

- ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts
- ensuring that personal information being transferred electronically is encrypted
- ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software
- performing regular IT audits to ensure that the security of the organisation's hardware and software systems are functioning properly
- performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons

8.4 Marketing & communication manager

See the service agreement with the external marketing provider who is responsible for:

- approving and maintaining the protection of personal information statements and disclaimers that are displayed on the organisation's website, including those attached to communications such as emails and electronic newsletters
- where necessary, working with persons acting on behalf of the organisation to ensure that any outsourced marketing initiatives comply with POPIA

8.5 Employees and others acting on behalf of Finfocus

Employees acting on behalf of Finfocus will, during the course of performing their duties, gain access to the personal information of clients. Employees are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties.

Employees and other persons acting on behalf of the organisation must request assistance from their Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will only process personal information where:

- the data subject, or a competent person where the data subject is a child, consents to the processing; or
- the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- the processing complies with an obligation imposed by law on the responsible party; or
- the processing protects a legitimate interest of the data subject; or
- the processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied

Furthermore, personal information will only be processed where the data subject:

- clearly understands why and for what purpose his, her or its personal information is being collected; and
- has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the organisation will under no circumstances:

- process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties
- save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server
- share personal information informally

Employees and other persons acting on behalf of the organisation are responsible for:

- keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy
- ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created
- ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons
- ensuring that computer screens and other devices are switched off or locked when not in use or when away from their desks
- ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used
- ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet
- ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer
- taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, proof of that the updated information is correct must be supplied by the data subject
- taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected and in terms of regulatory requirements. Where personal information is no longer required, authorisation must first be

obtained from the Information Officer to delete or dispose of the personal information in the appropriate manner
- undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

9. POPI AUDIT

The information officer will schedule periodic POPI audits, the purpose of which is to:

- identify the processes used to collect, record, store, disseminate and destroy personal information
- determine the flow of personal information throughout Finfocus
- define the purpose for gathering & processing personal information
- ensure the processing parameters are still adequately limited
- ensure that new data subjects are made aware of the processing of their personal information
- re-establish the rationale for any further processing where information is received via a third party.
- verify the quality and security of personal information.
- monitor the extend of compliance with POPIA and this policy.
- monitor the effectiveness of internal controls established to manage the organisation's POPI related compliance risk

In performing the POPI Audit, Information Officer will attempt to identify areas within in the organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information. The Finfocus information officer has direct access to the Finfocus Client Relationship Management system and will be able to monitor POPIA compliance on an ongoing basis

10. Request to access personal information procedure

Data subjects have the right to

- request what personal information the organisation holds about them and why
- request access to their personal information
- be informed how to keep their personal information up to date.

Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the organisation's PAIA Policy.

The Information Officer will process all requests within a reasonable time.

11. POPI complaints procedure

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The organisation takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to the organisation in writing. Where so required, the Information Officer will provide the data subject with a "POPI Complaint Form";
- where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day;

- the Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days;
- the Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA;
- the Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the organisation's data subjects;
- where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach;
- the Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the organisation's governing body within 7 working days of receipt of the complaint. In all instances, the organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

- The Information Officer's response to the data subject may comprise any of the following:
  - A suggested remedy for the complaint,
  - A dismissal of the complaint and the reasons as to why it was dismissed,
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

12. Disciplinary action

Where a POPI complaint or a POPI infringement investigation has been finalised, the organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, the organisation will undertake to provide further awareness training to the employee.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organisation may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.

***

Annexure A: Personal information request form

Please submit the completed form to the Information Officer:

Name: Schalk van Niekerk
Contact Number: 021 861 7000
Email Address: schalkvn@finfocus.co.za

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject

Name & Surname	
ID	
Postal	
Contact Number	
Email	

B. Request

I request the organisation to:	
(a) Inform me whether it holds any of my personal information	☐
(b) Provide me with a record or description of my personal information	☐
(c) Correct or update my personal information	☐
(d) Destroy or delete a record of my personal information	☐

C. Instructions

Signature _____ **Date** _____

Annexure B: POPI complaint form

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please submit the completed form to the Information Officer:

Name: Schalk van Niekerk
Contact Number: 021 861 7000
Email Address: schalkvn@finfocus.co.za

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator.

The Information Regulator: Ms Mmamoroke Mphelo
Physical Address: SALU Building, 316 Thabo Sehume Street, Pretoria
Email: inforreg@justice.gov.za
Website: http://www.justice.gov.za/inforeg/index.html

A. Particulars of complainant

Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

B. Details of complaint

C. Desired outcome

Signature _____ **Date** _____

Annexure C: POPI notice and consent form to allow access to personal information

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officers, Schalk van Niekerk, CFP® (Schalkvn@finfocus.co.za).

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our information officer's contact details

Name: Schalk van Niekerk
Contact Number: 021 861 7000
Email Address: schalkvn@finfocus.co.za

Purpose for processing your information

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- providing you with advice, products and services that suit your needs as requested
- to verify your identity and to conduct credit reference searches
- to issue, administer and manage your insurance policies
- to process insurance claims and to take recovery action
- to notify you of new products or developments that may be of interest to you
- To confirm, verify and update your details
- to comply with any legal and regulatory requirements

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Consent to disclose and share your information

We may need to share your information to provide advice, reports, analyses, products or services that you have requested.

Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa

Annexure D: SLA (service level agreement) confidentiality clause

- Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email 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 whether the information is recorded electronically or otherwise.

- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with, or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.

- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.

- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.