1.618
advisory services

Popia Policy 2026

1.618 Advisory Services PTY Ltd
FSP 18147 • Registration No. 2012/115015/07 • VAT No. 4070262623
Directors: Candice Giles | Tyrone Hodgson

1. VERSION CONTROL

The Responsible Party undertakes to review this policy regularly.

Version number	Version date	Summary of changes made
1	July 2021	These initial regulations outlined
2	May 2025	Form 1, Form 3 and Form 4 added
3	March 2026	Health Regulations
4		

Registered Information Officer:

Heidi Ludeke

Registered Deputy Information Officer

Elmari Gates

2. CONTENTS

3. DEFINITIONS

"1.618" or **"we"** refers to 1.618 Financial Services (Pty) Ltd registration number 2010/009412/07 with domicilium citandi et executandi at Building 3, 1st Floor, Block C, Blueberry Office Park, Apple Road, Randpark Ridge, Johannesburg, 2194.

"Data Subject" means any person whether natural or juristic who has provided us with information or from whom we have collected information

"Personal Information" means facts of a distinctive and confidential nature provided by or collected from an identifiable, living, natural person, and/or an identifiable, existing juristic person for purposes of assisting 1.618 in rendering a service to the client. Personal information may refer to records owned, held or otherwise under control of 1.618. Including, but not limited to—

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- 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; and
- 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;
- Personal information concerning a child.

"Processing" means any operation or activity, whether or not by automatic means, including but not limited to collection, receipt, storage, update, modify, retrieval, use, merge, link, restrict, degrade, erase, transmit or distribute.

"IO" or **"Information Officer"** means the person designated to handle complaints and requests in terms of this policy or any of the information that 1.618 processes, so mandated in terms of Paragraph 11 of this policy.

Third Party Operator means a person (natural or legal) who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

Health Information means the personal information relating to a data subject's physical or mental health, including information arising from healthcare services, testing, treatment or diagnosis.

4.INTRODUCTION

1.618 Financial Services (Pty) Ltd is a boutique financial services company who pride themselves on providing a holistic solution for each client. The Protection of Personal Information Act 4 of 2013 requires that we keep you informed on how we use your information, for what purpose we collect and use your information, and how long we intend to keep it. We are committed to protecting our clients' privacy and will collect and use your information minimally, transparently, and for the purpose for which it was collected.

1.618 is committed to keeping your information safe and secure, to provide you with reasonable access to your information, and to give effect to your rights in terms of POPI and the ECTA. To this extent, we emphasise that your information is collected only by necessity, used accordingly, and that it is necessary to protect your legitimate financial interests.

5. APPLICATION OF THIS POLICY

The obligations in this policy apply to 1.618, its management, staff members, and representatives. Any Third Parties who 1.618 entrusts personal information to are also bound by the terms in this policy. It applies to all Personal Information gathered from Data Subjects.

6. LEGAL BASIS

Any information that we collect from you will be done with your consent. Consent will be obtained from our clients during negotiations, introductory meetings, initial briefs or a preliminary stage of analysis. If we are mandated by law to collect your information, we will notify you of the authorising law.

Where you provide us with information, you do so willingly and voluntarily with the understanding that we require the information to pursue both our clients' legitimate interests as well as our own.

To carry on business and to protect your interests, we require your information and will treat it with the utmost confidence- but should you at any time during the processing of your information object to the same, you may withdraw your consent by giving us reasonable notice.

7. PURPOSE OF COLLECTION

1.618 requires certain categories of information (more info in paragraph 4 below) to ensure that you receive the quality service you have come to expect, and that your needs are met. Information may be collected for explicitly defined purposes or incidental to the function, activity or service of 1.618 or a responsible third party.

The purpose of collecting your information includes, but is not limited to:

- Providing financial advice and intermediary services
- Providing any value added products or service to enable your financial wellbeing

1.618 warrants that your information will never be used for a reason not in line with what it was collected for. Should the purpose we collect your information not be specified in this paragraph, the purpose will be communicated to you in writing and agreed to.

8. CONSENT

Any information that we collect from data subjects will be with consent. The rule of thumb is if the business is collecting information from any person whether natural or legal it must obtain a signed Consent Form. Consent may be obtained from data subjects during introductory meetings, application forms, electronic media or ongoing interaction. It might also be via online website cookies or any other form of valid consent.

Where data subjects provide us with information, the need to do so willingly and voluntarily with the understanding that we require the information to pursue both our clients' legitimate interests as well as our own.

To carry on business and to protect or facilitate data subject interests, we require personal information from time to time and will treat it with utmost confidentiality. should a data subject at any time during the processing of their information object to same, they may withdraw consent by furnishing us with reasonable notice and in the prescribed form attached.

9. INFORMATION WE REQUIRE

1.618 collects different categories of information from our clients depending on their financial needs. We do not collect information that is excessive or irrelevant to the purpose specified, striving to collect only the information that is necessary for us to deliver our service and to comply with financial services law.

To the extent we require information from you, you can expect to provide us with information including but not limited to:

- full names and surnames;
- postal and/or physical addresses;
- identity number of the client;
- contact details:
    - email Addresses;
    - telephone Numbers;
    - mobile Phone Numbers; and/or
    - fax Numbers
- Financial Needs
- Assets
- Liabilities
- Estate information
- Property information
- Health information
- and any other information that may be necessary to enable us to provide you with our service.

Please bear in mind that this is not an exhaustive list and we may at times require information that is not contained herein. We will inform our clients as to the information we collect from them whenever practicable, whether such information is voluntary or mandatory, and what the consequences are if information is not provided (both in cases of mandatory and voluntary collection).

10. HOW WE SHARE YOUR INFORMATION

1.618 staff are regularly reminded that they have a confidentiality obligation towards our clients who hold a Right to Privacy under the Constitution, and neither 1.618 nor its staff will disclose your information to a third party unless:

- we are required to do so by law; or
- the disclosure is necessary to enable us to perform our functions as per our clients' mandates; or
- it is vital to protecting the rights of 1.618.

In the event that your information is to be disclosed to a third party, 1.618 will ensure that the third party receiving your information is as committed to protecting your privacy and information as we are.

11. ACCESS TO AND INTEGRITY OF INFORMATION

1.618 is committed to maintaining the integrity and accuracy of your information. To this extent, clients are reminded that they may request access to their own information at any time and to request that we update or correct any information that may be outdated or incorrect.

We take reasonable and routine steps to ensure that the information we collect is up to date and accurate. Where information does not need to be updated to fulfil the purpose for which it was collected, such information will not be updated without the client's express request.

1.618 provides for four categories of requestors for access to information:

- a person requesting his or her own information;
- a person requesting information for and on behalf of another person;
- a person requesting information about another person; or
- a public body that requests information in the public interest

Requestors must provide proof of identity and a Power of Attorney where applicable. 1.618 may request any other information to verify the requestor's identity.

12. SECURITY OF INFORMATION

The safety and confidentiality of your information is of paramount importance to 1.618 and its staff. To this extent, 1.618 is committed to preventing unauthorized access, damage, loss of, or destruction of your information by ensuring industry appropriate and adequate security measures are implemented and persistently reviewed.

1.618 maintains strict security and confidentiality measures for both physical and electronic health records. The processing of health information is subject to a strict duty of confidentiality and outline procedures for the secure, permanent disposal of these specific records.

We do our best to identify risks both internal and external and to adapt accordingly we implement security systems with due regard to generally accepted information security practices.

Where there are reasonable grounds to suspect that the personal information of a data subject has been breached (accessed, acquired, deleted or damaged by an unauthorised third party), we will notify the data subject of such a breach as well as inform the information regulator as soon as reasonably possible after the breach is discovered.

13. HOLDING PERIODS

Information we collect on data subjects will not be held for longer than necessary, or if the purpose for which said information was collected has ultimately been fulfilled, or if the collected information has become obsolete.

Where no agreements, other laws or terms in this policy apply, a record of personal information will be kept for one year after the information was finished being processed, including usage for the specific purpose for which the information was collected originally.

We will destroy Records of Personal Information as soon as reasonably practicable, unless further retention is required by the laws mentioned above or agreed to between the parties.

For more information on durations of specific records, please refer to Annexure A to view our Record Retainment Policy.

14. ERASURE OF INFORMATION

1.618 will endeavour that information be destroyed, where reasonable, after its retention period has lapsed in terms of paragraph 8.

If paragraph 8 does not apply, clients are reminded that they have the right to obtain the erasure of their personal data without an undue delay if:

- the information is no longer necessary for the specified purpose it was collected for; or
- where the data subject withdraws consent in terms of paragraph 2 of this policy; or
- the collected personal information is inaccurate, irrelevant, excessive or incomplete.

If clients prefer for 1.618 to cease processing their information instead of deleting it, reasonable notice may be given to this effect following which we will immediately stop processing your information.

15. DIRECT MARKETING

We will never process your information for the purpose of direct marketing (or spam) unless Data Subjects:

- have consented to such processing; or
- had not previously refused consent; and if
- contact details were obtained in the context of providing them with our services; and if
- they were given reasonable opportunity to object to the direct marketing; or
- was already a data subject

16. EMPLOYEE HEALTH DATA

In addition to general personal information, The Responsible Party acknowledges its specific obligations as an employer regarding the processing of employee Health Information. We strictly limit the collection and processing of employee health data to what is legally mandated and practically necessary for employment and health and safety purposes.

The specific employee Health Information we may collect includes, but is not limited to:

- Sick notes and medical certificates.
- Occupational health and safety records.
- Medical scheme or health insurance details.

This information is collected and processed solely for the following justifiable purposes:

- Fulfilling statutory and contractual leave requirements (such as administering sick leave).
- Facilitating emergency medical procedures and ensuring workplace safety.
- Administering employee benefits related to healthcare.

All employee Health Information is treated as highly confidential, subject to the strict security measures and permanent disposal procedures outlined in Section 5.5 of this policy

17. SECURITY MEASURES

1.618 staff are regularly reminded that they have a confidentiality obligation towards data subjects who hold a Right to Privacy under the Constitution, and neither The Responsible Party nor its staff will disclose data subject information to a third party unless:

- we are required to do so by law; or
- the disclosure is necessary to enable us to perform our functions as per our clients' mandates; or
- it is vital to protecting the rights of the Responsible Party

18. AUTHORITY

In the event that information is to be disclosed to a third party, The Responsible Party will ensure that the third party receiving personal information is as committed to protecting your privacy and information as we are. We do this via obtaining a commitment form from the third party in written form where the third party agrees to keep information confidential and maintains security measures.

We disclose information to third parties such as:

- Link Up ICT (Pty) Ltd
- Bitco
- Liquid Telecommunications
- Konica Minolta
- Cloud on Demand
- Securecom

19. DATA BREACH MANAGEMENT

A Data Breach incident is an event that has caused or can potentially cause damage to our organisation's assets, reputation and / or personnel which includes our customers and any other personal information we process, store or share. A Data Breach can occur when there is intrusion, compromise and misuse of information by a party that does not have lawful access rights to the information that was compromised.

An Information Security Incident includes, but is not restricted to, the following;

- The illegitimate use of our systems for the processing, storage or sharing of data by any person.
- The transfer of personal information to persons who are not entitled to receive that information.
- The loss or theft of personal and/or classified data and information via any means, for example hacking or even attempted hacking.
- Unauthorised changes to personal information via our system hardware or software.
- Unauthorised disruption or denial of service to our system.

Where there are reasonable grounds to suspect that the personal information of a data subject has been breached (accessed, acquired, deleted or damaged by an unauthorised third party), we will:

- notify the data subject of such a breach in detail, as well as
- inform the information regulator as soon as reasonably possible after the breach is discovered.

Data breach communication to the data subject can be done in one of the following methods:

- 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; or
- As may be directed by the Regulator.

The communication must include enough information so that the data subject can take protective measures and should include:

- A description of the possible consequences of the breach;
- A description of the measures that the responsible party intends to take or has taken to address the security breach;
- A recommendation with regard to the measures to be taken by the data subject
- To mitigate the possible adverse effects of the breach; and
- If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

Any data breaches experienced by Third Party Operators must be reported to the Responsible Party.

20. PROHIBITED DATA PROCESSING ANS EXEMPTIONS

Due to the nature of our business we may from time to time obtain data that is prohibited to enable us to offer our services and to comply with the laws applicable to our business. As such we aim to make use of the exemptions that the POPI Act provides in instances where the information is needed. We obtain consent for this personal information and may include but not be limited to:

- The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, sex life or biometric information of a data subject (Note: Exemptions for Health Information

are governed specifically by our internal safeguards and the 2026 Health Information Regulations as outlined in Sections 5.5 and 5.9) ; or

- The criminal behaviour of a data subject to the extent that such information relates to-
    - The alleged commission by a data subject of any offence; or
    - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- Personal information concerning a child.

21. INFORMATION OFFICER

1.618's Information Officer is responsible for:

11.1 Ensuring information policies are reviewed, up to date and sufficient;

11.2 Handling complaints or requests made in terms of this policy;

11.3 Supporting this policy with relevant documentation;

11.4 Ensuring Information Security training is conducted;

11.5 Backing up data;

11.6 Reporting incidents and allocating security responsibilities; and

11.7 Any other relevant information-related duty or responsibility.

1.618's Information Officer is **Heidi Ludeke:**

Contact: 011 068 6600

Email: heidi@1618.co.za

22. PERSONAL INFORMATION TRANSFERS OUTSIDE SOUTH AFRICA

Due to the pervasive and widespread use of cloud technology and the disappearance of national borders in the broader context of the digital age we live in it is accepted that Personal Information of Data Subjects will almost always be transferred internationally. It is not always possible to pinpoint exactly in which country the cloud service is hosted as this may change from time to time as data centres operate internationally in several countries. It may well be the case that Personal Information is transferred to multiple countries.

The use of these services are required to be able to operate as a business, to stay competitive and to keep up to date with new digital technological innovation. We also require the use of these services to be able to provide clients with our services.

For all Data Subjects we obtain consent to transfer their information across borders and this is to be done before we do so.

Notwithstanding the general provisions above, the transfer of Health Information to a third party in a foreign country is subject to heightened restriction. 1.618 strictly prohibits the transfer of Health Information across borders (including storage via international cloud providers) unless the requirements of **Section 72(1) of POPIA** are fully satisfied.

Specifically, Health Information will only be transferred if:

- The recipient is subject to a law, binding corporate rules, or a binding agreement which provides an **adequate level of protection** substantially similar to the conditions for lawful processing as set out in POPIA; or
- The Data Subject explicitly consents to the transfer; or

- The transfer is necessary for the performance of a contract between the Data Subject and 1.618.

We will conduct due diligence to ensure that any cloud provider or third party handling Health Information is legally bound by data protection standards that meet these criteria.

The reasons or platforms we use to transfer Personal Information across borders are

- Cloud services for data file storage such as Dropbox, OneDrive etc.
- Cloud server services for email.
- Newsletter service providers.
- Proprietary software services and client CRM

23. FORMS

For Data Subjects to exercise their rights in terms of their information we need to abide by the law. In this context there are certain prescribed forms by POPI to be used when interacting with data subjects. Please see attached the forms for general use.

Form 2: Request for Correction or Deletion of Personal Information

Form 3: Application for the issue of a Code of Conduct

Form 4: Application for the Consent

24. POPIA AWARENESS

The responsible Party conducts POPI awareness sessions with all staff or other consultants or contractors via awareness sessions. All previously mentioned persons will be required to have completed the POPI awareness training.

From time to time more in-depth POPI awareness sessions may be held with the Information Officers and Deputy Information Officers.

25. SIGNATURES

As authorised signatory of the Responsible Party I, Candice Samantha Giles hereby confirm official adoption of this policy.

DIRECTOR
Candice Giles

_____

INFORMATION OFFICER
Heidi Ludeke

_____