DATA PROTECTION POLICY

VERSION 1.02

THE PRIME FINANCIAL SERVICES GROUP
28 PETER PLACE
LYME PARK
SANDTON
2060

CONTENTS

1. SCOPE OF THE POLICY 3

2. PURPOSE AND RATIONALE OF THE POLICY 3

3. DEFINITIONS 3

4. DATA PROTECTION PRINCIPLES 6

LAWFUL PROCESSING OF PERSONAL INFORMATION 6

ACCOUNTABILITY 6

PROCESSING LIMITATION 7

PURPOSE SPECIFICATION & LIMITATION 7

FURTHER PROCESSING LIMITATION 8

STORAGE LIMITATION 8

INFORMATION QUALITY 8

OPENNESS, FAIRNESS & TRANSPARENCY 8

SECURITY SAFEGUARDS 9

DATA SUBJECT PARTICIPATION 9

THE CONDITIONS FOR PROCESSING THE PERSONAL AND SPECIAL PERSONAL INFORMATION OF A CHILD . 9

5. RIGHTS OF DATA SUBJECTS 10

THE RIGHT TO BE NOTIFIED 10

THE RIGHT TO ACCESS 10

THE RIGHT TO REQUEST THE CORRECTION, DESTRUCTION OR DELETION 11

THE RIGHT TO OBJECT 11

THE RIGHT TO SUBMIT A COMPLAINT AND/OR INSTITUTE CIVIL PROCEEDINGS 11

RESTRICTIONS 11

REQUESTS PROCEDURE 11

6. DATA PROCESSING BY THE GROUP 12

COLLECTION OF PERSONAL INFORMATION 12

THE PERSONAL INFORMATION WE COLLECT 12

SENSITIVE PERSONAL INFORMATION 13

HOW WE USE THE PERSONAL INFORMATION 13

SHARING OF PERSONAL INFORMATION 13

SHARING OF PERSONAL INFORMATION ABROAD 14

CONFIDENTIALITY OF PERSONAL DATA 14

SECURITY OF PERSONAL DATA 14

PERSONAL INFORMATION BREACH 15

Reporting personal information breaches to officer 15

Reporting personal information breaches to Regulator 15

DATA PROTECTION IMPACT ASSESSMENTS 15

PERSONAL DATA RETENTION 16
7. DATA PROCESSING BY IMPLEMENTING PARTNERS 16
GENERAL CONDITIONS 16
VERIFICATION 16
PARTNERSHIP AGREEMENTS 16
PARTNERSHIP TERMINATION 16
8. TRANSFER OF PERSONAL DATA TO THIRD PARTIES 17
GENERAL CONDITIONS 17
DATA TRANSFER AGREEMENTS 18
9. ACCOUNTABILITY AND SUPERVISION 18
DATA PROTECTION OFFICER 18
DATA CONTROLLER 19
10. CHANGES TO THIS POLICY 19
ANNEXURE 1: OWNERSHIP, APPROVAL & REVISION HISTORY 20
POLICY OWNER 20
POLICY APPROVAL 20
POLICY REVISION 20

1. SCOPE OF THE POLICY

1.1. This policy applies to the legal entities within the Prime Financial Services Group (hereinafter referred to as "the Group") as shown on the Group's corporate organogram and amended from time to time (excluding Automated Outsourcing Services (Pty) Ltd).

1.2. The policy applies to all employees of the Group. Compliance with this policy and the related policies and procedures is mandatory. Any breach of this policy and any related policies and procedures may result in disciplinary action. All employees must read, understand and comply with this policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

2. PURPOSE AND RATIONALE OF THE POLICY

2.1. During the course of business, the Group is often required to process personal data of persons. Due to the sensitive nature of the data that we might process, proper protection of the personal data are therefore of particular importance and the Group has a responsibility to process it in a way that respects data protection principles.

2.2. The purpose of the policy is to formally document the Group's commitment to compliance with the Protection of Personal Information Act (POPIA) of South Africa as amended from time to time as well as compliance with the requirements of any associated Data Protection legislation, including the General Data Protection Regulation (GDPR).

2.3. The policy sets out the rules and practises which must be followed when processing personal information of individuals and juristic persons (hereinafter "persons"), which includes employees, clients, suppliers and third parties.

2.4. The policy applies to all personal information that the Group processes, regardless of the format or media on which the data are stored or who it relates to.

2.5. The policy will be complemented by operational guidelines that will provide guidance on its implementation, supervision and accountability.

3. DEFINITIONS

3.1. ''**child"/"children**" 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 him- or herself;

3.2. ''**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;

3.3. "**Complaint**" means –

a) a matter reported to the Information Regulator in terms of section 74(1) and (2) of the Act;
b) a complaint referred to in section 76(1)(e) and 92(1) of the Act; and
c) a matter reported or referred to the Information Regulator in terms of other legislation that regulates the mandate of the Information Regulator.

3.4. "**complainant**" means any person who lodges a complaint with the Information Regulator;

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

3.6. ''**data subject''** means the person/individual to whom personal information relates;

3.7. "**data transfer arrangement**" means any API Agreement, Service Level Agreement, or any other agreement with a third party that might include the transfer of personal information;

3.8. "**day**" means a calendar day, unless the last day of a specified period happens to fall on a Sunday or on any public holiday, in which case the time shall be calculated exclusive of that Sunday or public holiday in accordance with section 4 of the Interpretation Act, 1957 (Act No. 33 of 1957);

3.9. "**de-identify**", in relation to personal information of a data subject, means to delete any information that – (a) identifies the data subject; (b) can be used or manipulated by areasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method ro other information that identifies the data subject, and "de-identified" has the same meaning.

3.10. ''**direct marketing''** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason;

3.11. ''**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;

3.12. ''**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;

3.13. "**GDPR**" means the General Data Protection Regulation 2016/679, a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

3.14. "**implementing partner**" means an organization established as an autonomous and independent entity from the Group that the Group engages through a partnership agreement. Where the collection and processing of personal data is one of the responsibilities of Implementing Partners and the personal data is being collected and processed on behalf of the Group.

3.15. "**officer"** means ''information officer'' or "data protection officer" of, or in relation to, a private body, appointed by the Group.

3.16. ''**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;

3.17. ''**personal information**'' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

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

h. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

3.18. ‘‘**POPIA’’** means the Protection of Personal Information Act, No. 4 of 2013 and includes any regulation or code of conduct made under the Act;

3.19. ‘‘**processing**’’ means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

a. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
b. dissemination by means of transmission, distribution or making available in any other form; or
c. merging, linking, as well as restriction, degradation, erasure or destruction of information;

3.20. ‘‘**Promotion of Access to Information Act**’’ means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

3.21. ‘‘**record**’’ means any recorded information—

a. regardless of form or medium, including any of the following:
   i. Writing on any material;
   ii. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
   iii. label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;
   iv. book, map, plan, graph or drawing;
   v. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

   in the possession or under the control of a responsible party;
b. whether or not it was created by a responsible party; and
c. regardless of when it came into existence;

3.22. ‘‘**Regulator**’’ means the Information Regulator established in terms of POPIA;

3.23. ‘‘**re-identify**’’, in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

a. identifies the data subject;
b. can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
c. can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ‘‘re-identified’’ has a corresponding meaning;

3.24. ‘‘**Republic**’’ means the Republic of South Africa;

3.25. ‘‘**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;

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

3.27. ‘‘**special personal information’’** means personal information as referred to in section 26 of POPIA; and

3.28. ‘‘**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.

4. DATA PROTECTION PRINCIPLES

LAWFUL PROCESSING OF PERSONAL INFORMATION

4.1. The Group is committed to comply with the conditions for the lawful processing of personal information by or for a responsible party that does not infringe the privacy of the data subject.

4.2. In order to collect and process personal information for any specific purpose, the Group must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by the Group.

4.3. In addition to the lawfull processing of personal information, the Group must respect and apply the basic principles when processing personal data, as set out below.

ACCOUNTABILITY

4.3.1. The Group is responsible for and must be able to demonstrate compliance with the data protection principles and all other obligations under the relevant data protection legislation. This is known as the 'accountability principle'.

4.3.2. The Group must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with its obligations in the terms of the relevant legislation, including:

a. Appointing a suitably qualified and experienced officer, and providing them with adequate support and resource;
b. Although an officer will be appointed, the Group must implement a strategy in terms whereof each department within the business takes responsibility for data protection compliance by that division, being accountable as a business unit;
c. Ensuring that at the time of deciding how the Group will process personal information, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles;
d. Ensuring that, by default, only personal information that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data;
e. Ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, the Group has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a Data Protection Impact Assessment (see clauses6.32 to 6.36);
f. Integrating data protection into the Group's internal documents, privacy policies and fair processing notices;
g. Regularly training the Group's staff on the relevant data protection legislation, this policy and the Group's related policies and procedures, and maintaining a record of training completion by members of staff;
h. Regularly testing the measures implemented by the Group and conducting periodic reviews to assess the adequacy and effectiveness of this policy, and the Group's Related policies and procedures;
i. The Group must keep full and accurate records of all its processing activities in accordance with the legislation requirements;
j. The Group must implement measures to keep individuals accountable for non compliance of this policy. Each business division and data controller need to take responsibility to ensure (and monitor) that the division implements the policy;

k. Each employee must ensure to take the necessary training providing by the Group and, where they are responsible for other members of staff, that they have done so;
l. Each employee must further review all the systems and processes under their control to ensure that same are adequate and effective for the purposes of facilitating compliance with the Group's obligations under this policy; and must ensure that you observe and comply with all policies and guidance which form part of the Group's Policy Framework.

PROCESSING LIMITATION

4.3.3. Processing of personal data may only be carried out for specified, explicit and legitimate purposes. The processing must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

Minimality

4.3.3.1. The personal data that the Group collects and processes must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

4.3.3.2. Each employee must only process personal data when necessary for the performance of their duties and tasks and not for any other purposes. Accessing personal data that he/she are not authorised to access, or that they have no reason to access, may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

4.3.3.3. An employee may only collect personal data as required for the performance of his/her duties and tasks and should not ask a data subject to provide more personal data than is strictly necessary for the intended purposes. An employee must ensure that when personal data are no longer needed for the specific purposes for which they were collected, that such personal data are deleted, destroyed or anonymised.

Consent and Justification

4.3.3.4. The Group may only process personal data based on one or more of the following legitimate bases:

a. the data subject or a competent person where the data subject is a child consents to the processing;
b. processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
c. processing complies with an obligation imposed by law on the responsible party;
d. processing protects a legitimate interest of the data subject;
e. processing is necessary for the proper performance of a public law duty by a public body; or
f. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

4.3.3.5. The data subject or competent person may withdraw his, her or its consent, as referred to above at any time, subject to clause 5.1.10.

PURPOSE SPECIFICATION & LIMITATION

4.3.4. The Group must only process personal information for one or more specific and legitimate purpose(s) (necessary and proportionate to the purpose(s) for which it is being processed) and it should not be processed in a way incompatible with this/those purpose(s).

4.3.5. The Group msut examine the extent of information that is required for the purpose as intended and ensure that we collect adequate and relevant information and prevent any excessive information collection.

FURTHER PROCESSING LIMITATION

4.3.6. The Group must ensure that the data shall not be further processed in any manner that is contrary to that purpose or the purposes for which the data were originally collected. Where the Group intends to do so, it must inform the data subject(s) before using their personal information for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

4.3.7. In additio to the above, the Group must ensure that personal information is not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

STORAGE LIMITATION

4.3.8. The personal data that the Group collects and processes must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected (except in order to comply with any legal, accounting or reporting requirements).

4.3.9. Storing personal data for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage.

4.3.10. The Group will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which they were collected.

4.3.11. Each employee must regularly review any personal data processed by him/her in the performance of their duties and tasks to assess whether the purposes for which the data were collected have expired. Where appropriate, an employee must take all reasonable steps to delete or destroy any personal data that the Group no longer requires.

4.3.12. All privacy notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

INFORMATION QUALITY

4.3.13. The Group must ensure that personal information are recorded as accurately as possible and, where necessary, updated to ensure it fulfils the purpose(s) for which it is processed.

4.3.14. Each employee must ensure that they update all relevant records if they become aware that any personal information are inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

OPENNESS, FAIRNESS & TRANSPARENCY

4.3.15. The Group must ensure that all personal information are processed lawfully, fairly and in a transparent manner.

SECURITY SAFEGUARDS

4.3.16. The Group must maintain the confidentiality of the personal data of persons of concern at all times, even after a data subject is no longer of concern to the Group. The Group must ensure that personal information are processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.3.17. In order to ensure the confidentiality and integrity of personal information, appropriate technical and organizational data security measures need to be put in place.

4.3.18. The Group has developed, implemented and will maintain appropriate technical and organisational measures for the processing of personal data taking into account the; nature, scope, context and purposes for such processing; volume of personal data processed and likelihood and severity of the risks of such processing for the rights of data subjects.

4.3.19. The Group will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

4.3.20. Each employee is responsible for ensuring the security of the personal information processed by him/her in the performance of their duties and tasks. Each employee must ensure that they follow all procedures that the Group has put in place to maintain the security of personal information from collection to destruction.

4.3.21. Each employee must ensure that the confidentiality, integrity and availability of personal information are maintained at all times:

a. Confidentiality: means that only people who need to know and are authorised to process any personal data can access it
b. Integrity: means that personal data must be accurate and suitable for the intended purposes
c. Availability: means that those who need to access the personal data for authorised purposes are able to do so.

4.3.22. Employees must ensure to observe and comply with our Information Security Policy. Employees must not attempt to circumvent any administrative, physical or technical measures the Group has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

4.3.23. Reporting of personal information breaches are dealt with in clauses 6.27 to 6.31.

DATA SUBJECT PARTICIPATION

4.3.24. The data subjects rights are dealt with under Section 5 of the policy.

THE CONDITIONS FOR PROCESSING THE PERSONAL AND SPECIAL PERSONAL INFORMATION OF A CHILD

4.3.25. The Group recognises that children are vulnerable. Processing the personal information of children is prohibited unless one of the following justifications are present:

a. A parent or guardian can consent (“parental consent”) to the processing;

b. The processing is necessary for the establishment, exercise or defence of a right or obligation in law (which includes obligations of international public law). In the case of a contract, the child would need parental consent to validly conclude a contract;
c. The personal information is being used for historical, statistical or research purposes if it services a public interest and it is impossible (or would require a disproportionate effort to ask for consent). Where this is necessary, the Group must provide sufficient guarantees that the privacy of child is not disproportionately affected. In most cases Group would rather attempt to de-identify the information.
d. The prohibition also does not apply if the child deliberately made the personal information public with the consent of a parent or guardian.

4.3.26. The following scenarios are instances where parental consent should be obtained:

a. Where the child's personal information is going to be disclosed to a third party;
b. If the child's details is going to be used for marketing purposes;
c. If the information is going to be made public;
d. If the child's image is going to be used on a website which is open to the public;
e. Where the child is going to be asked for personal information of third parties like family members or friends.

5. RIGHTS OF DATA SUBJECTS

5.1. A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Section 4, including the following:

THE RIGHT TO BE NOTIFIED

5.1.1. A data subject has the right to be notified when their personal information is collected.

5.1.2. When collecting personal data from a data subject, the Group must inform the data subject of the following, in writing or orally, and in a manner and language that is understandable to the data subject:

a. The specific purpose(s) for which the personal data or categories of personal data will be processed;
b. Whether such data will be transferred to third parties or, where the data is being collected by a third party on behalf of the Group, that the data subject is informed of this fact;
c. The importance of the data subject providing accurate and complete information;
d. The data subject's duty to keep the Group, and/or, as appropriate, third parties, informed of changes to their personal situation;
e. Any consequences for refusing or failing to provide the requested personal data;
f. The data subject's right to request access to their personal data, or correction or deletion of it;
g. The data subject's right to object to the collection ofpersonal data and the practical consequences thereof;
h. How to lodge a complaint with the Regulator and inform the data subject of its right to institute legal proceedings.

THE RIGHT TO ACCESS

5.1.3. A data subject has the right to establish whether the Group or any of our third parties hold its personal information and to request access thereto. Please note that any such access request may be subject to a payment of a legally allowable fee.

THE RIGHT TO REQUEST THE CORRECTION, DESTRUCTION OR DELETION

5.1.4. Subject to clause 5.1.10, a data subject may request the correction or deletion of personal data that is inaccurate, incomplete, unnecessary or excessive.

5.1.5. Where a data subject requests the correction or deletion of his or her personal data, the Group will request proof relating to the inaccuracy or incompleteness.

THE RIGHT TO OBJECT

5.1.6. Subject to section , a data subject has the right to object, in the prescribed manner, on reasonable grounds relating to its particular situation to the processing of its personal information, unless legislation provides for such processing.

5.1.7. If a data subject has objected to the processing of personal information and the objection is justified, the Group and/or any of our third parties may no longer process the personal information.

THE RIGHT TO SUBMIT A COMPLAINT AND/OR INSTITUTE CIVIL PROCEEDINGS

5.1.8. A data subject has the right to submit a compliant to the regulator or institute civil proceedings regarding the alleged interference with the protection of the personal information of any data subject.

5.1.9. If a data subject wants to submit a compliant, please refer to the Group's Complaints Resolution Policy.

RESTRICTIONS

5.1.10. The Group may refuse to provide a response or limit or restrict its response to a request or objection under Section 5 where:

a. It would constitute a necessary and proportionate measure to safeguard or ensure one or more of the following:

i. The safety and security of the Group, its personnel or the personnel of Product Providers, Implementing Partners and or any applicable third parties; or
ii. The overriding operational needs and priorities of the Group in pursuing its mandate and/or any regulatory requirements.

b. There are grounds for believing that the request is manifestly abusive, fraudulent or obstructive to the purpose of processing.

REQUESTS PROCEDURE

5.1.11. Requests for information about access to, correction or deletion of personal data or an objection, may be made by the data subject or his or her authorized legal representative, or, in the case of a child, a parent or legal guardian. Requests are to be submitted in writing to the following e-mail address: info@primeinvestments.africa

5.1.12. Before complying with any request or objection, the Group should satisfy itself of the identity of the person making the request or objection. The individual is required to identify him or herself in an appropriate manner. In the case of a legal representative or legal guardian, proof of such legal authority needs to be supplied. Requests and

objections from parents or guardians for children should be evaluated against the best interests of the child.

6. DATA PROCESSING BY THE GROUP

COLLECTION OF PERSONAL INFORMATION

6.1. The Group may collect or obtain personal information about data subject(s) –

a. directly from a data subject;
b. in the course of our relationship with a data subject;
c. in the course of providing services to a data subject;
d. when a data subject make his/her/its personal information public;
e. when a data subject visit and/or interact with our website or any of our social media platforms;
f. when a data subject register to use any of our services including but not limited to newsletters, seminars, training and legal updates;
g. when a data subject visit our offices.

6.2. The Group may also receive personal information about a data subject from third parties (eg, law enforcement authorities).

6.3. In addition to the above, the Group may create personal information about a data subject such as records of his/her/its communications and interactions with us, including, but not limited to, a data subject's attendance at events or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with a data subject during the course of our digital marketing campaigns.

THE PERSONAL INFORMATION WE COLLECT

6.4. The Group may process the following categories of personal information about a data subject:

a. personal details: full name;
b. demographic information: gender; date of birth / age; nationality; salutation; title; and language preferences;
c. identifier information: passport or national identity number; utility provider details; bank statements; tenancy agreements;
d. contact details: correspondence address; telephone number; email address
e. attendance records: details of meetings and other events organised by or on behalf of the Group that a data subject have attended;
f. consent records: records of any consents a data subject may have given, together with the date and time, means of consent and any related information;
g. payment details: billing address; payment method; bank account number or credit card number; invoice records; payment records; SWIFT details; IBAN details; payment amount; payment date; and records of cheques;
h. data relating to your visits to our website: your device type; operating system; browser type; browser settings; IP address; language settings; dates and times of connecting to a Website; and other technical communications information;
i. employer details: where you interact with us in your capacity as an employee of an organisation, the name, address, telephone number and email address of your employer, to the extent relevant; and
j. content and advertising data: records of your interactions with our online advertising and content, records of advertising and content displayed on pages displayed to you, and any interaction you may have had with such content or advertising (including, but not limited to, mouse hover, mouse clicks and any forms you complete).

SENSITIVE PERSONAL INFORMATION

6.5. Where we need to process your sensitive personal information, we will do so in the ordinary course of our business, for a legitimate purpose, and in accordance with applicable law.

HOW WE USE THE PERSONAL INFORMATION

6.6. Personal information is used as is appropriate in the normal course of business to provide the products and services that have been requested. We will primarily use your personal information only for the purpose for which it was originally or primarily collected.

6.7. We will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which the personal information was collected.

6.8. We may subject your personal information to processing during the course of various activities, including, without limitation, the following –

a. operating our business;
b. analysis, evaluation, review and collation of information in order to resolve any issues and potential disputes, prepare or comment on agreements, correspondence, reports, publications and other documents and records (whether in electronic or any other medium whatsoever);
c. compliance with applicable law and fraud prevention;
d. transfer of information to our Service Providers and other third parties; or
e. recruitment.

6.9. We may process your personal information for relationship management and marketing purposes in relation to our services (including, but not limited to, processing that is necessary for the development and improvement of our financial, investment and related services), for accounts management, and for marketing activities inorder to establish, maintain and/or improve our relationship with you and with our Service Providers. We may also analyse your personal information for statistical purposes.

6.10. We may process your personal information for internal management and management reporting purposes, including but not limited to: conducting internal audits, conducting internal investigations, implementing internal business controls, providing central processing facilities, for insurance purposes and for management reporting analysis.

6.11. We may process your personal information for safety and security purposes.

6.12. The Group may retain any information for purposes of investment transaction processing and administration, to monitor our website or to communicate directly with you.

SHARING OF PERSONAL INFORMATION

6.13. All personal information supplied to and/or collected by the Group is kept strictly confidential.

6.14. The Group will disclose or report personal information if and when required to do so by law or any regulatory authority, to its employees, and to its partners or agents who require such information to carry out their duties.

6.15. Employees are not permitted to share personal data with third parties unless the Group has agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, the Group has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the relevant legislation requirements for such agreements.

6.16. The transfer of any personal data to an unauthorised third party would constitute a breach of the lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach.

6.17. Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply.

6.18. For more information on data sharing to Implementing Partners and Third Parties, please refer to Section 7 and Section 8 respectively.

SHARING OF PERSONAL INFORMATION ABROAD

6.19. We may transfer your personal information to recipients outside of the Republic.

6.20. Personal information may be transferred outside of the Republic provided that the country to which the data is transferred has adopted a law that provides for an adequate level of protection substantially similar to POPIA and the GDPR, the Operator/third party undertakes to protect the personal information in line with applicable data protection legislation and the transfer is necessary in order to provide the financial en investment and other related services that are required by the Group's data subjects.

CONFIDENTIALITY OF PERSONAL DATA

6.21. Personal data is by definition classified as confidential. The confidentiality of personal data must be respected by the Group when processing personal data at all times.

6.22. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that it is accessible only to authorized personnel and transferred only through the use of protected means of communication.

SECURITY OF PERSONAL DATA

6.23. The Group is legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access and use of personal information. We will, on an on-going basis, continue to review our security controls and related processes to ensure that your personal information remains secure.

6.24. Our security policies and procedures cover:

k. Physical security;
a. Computer and network security;
b. Access to personal information;
c. Secure communications;
d. Security in contracting out activities or functions;
e. Retention and disposal of information;
f. Acceptable usage of personal information;
g. Governance and regulatory issues;
h. Monitoring access and usage of private information;
i. Investigating and reacting to security incidents.

6.25. When we contract with third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that personal information that we remain responsible for, is kept secure. Please refer to Section 8 for more detailed information.

6.26. We will ensure that anyone to whom we pass your personal information agrees to treat your information with the same level of protection as we are obliged to.

PERSONAL INFORMATION BREACH

Reporting personal information breaches to officer

6.27. The Group's staff are required to notify the applicable data controller and officer as soon as possible upon becoming aware of a personal data breach and to properly record the breach.

6.28. If a personal data breach is likely to result in personal injury or harm to a data subject, the officer should use his or her best efforts to communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay.

6.29. If an employee know or suspect that a personal information breach has occurred, he/she must contact the applicable data controller and officer immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach.

6.30. The breach notification should describe:

a. The nature of the personal data breach, including the categories and number of data subjects and data records concerned;
b. The known and foreseeable adverse consequences of the personal data breach; and
c. The measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the personal data breach.

Reporting personal information breaches to Regulator

6.31. In certain circumstances, relevant legislation will require the Group to notify the regulator, and potentially data subjects, of any personal information breach. The Group has put in place appropriate procedures to deal with any personal data breach and will notify the regulator and/or data subjects where the Group is legally required to do so.

DATA PROTECTION IMPACT ASSESSMENTS

6.32. A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data.

6.33. When elaborating new systems, projects or policies or before entering into data transfer arrangements with Implementing Partners or third parties which may negatively impact on the protection of personal data of persons of concern, the Group needs to carry out a DPIA.

6.34. A DPIA is required where the collection and processing or transfer of personal data is likely to be large, repeated or structural (i.e. where data is shared with an Implementing Partner or third party over a certain period of time). In practice, the Group requires a DPIA for any projects involving the use of personal data, including new systems, solutions and some research studies.

6.35. A DPIA must:

a) describe the nature, scope, context and purposes of the processing
b) assess necessity, proportionality and compliance measures
c) identify and assess risks to individuals
d) identify any additional measures to mitigate those risks.
e) DPIAs need to be assessed and signed off by the officer and, where relevant, IT Services.

6.36. The officer are responsible for organising and carrying out DPIAs, when required. DPIAs are normally carried out at the country level unless it is decided that a DPIA is to be carried out at global or regional level due to the scope of system or arrangement.

PERSONAL DATA RETENTION

6.37. Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purpose(s) for which it was collected.

6.38. All individual case files, whether open or closed, are considered permanent records, and must therefore be permanently retained in line with the Group's Retention Policy.

7. DATA PROCESSING BY IMPLEMENTING PARTNERS

GENERAL CONDITIONS

7.1. Where the collection and processing of personal data is one of the responsibilities of Implementing Partners, the personal data is being collected and processed on behalf of the Group. For these reasons, Implementing Partners are expected to respect and implement the same or comparable standards and basic principles of personal data protection as contained in this Policy.

7.2. This applies whether the Group intends to transfer personal data to Implementing Partners or Implementing Partners collect personal data in order to carry out agreed activities.

VERIFICATION

7.3. Irrespective of a partnership agreement, the Group needs to verify, prior to transferring personal data to an Implementing Partner or to engaging an Implementing Partner in the collection and processing of personal data, that the processing of personal data by the Implementing Partner satisfies the standards and basic principles of this Policy.

7.4. Such verification may form part of a DPIA.

PARTNERSHIP AGREEMENTS

7.5. The Group is to require Implementing Partners to comply with this Policy through an undertaking as part of the signing of partnership agreements. Such agreements also need to specify the specific purpose(s) for the processing of personal data and the legitimate basis for processing.

7.6. The Group may need to assist Implementing Partners in building or enhancing their capacity in order to comply with the data protection standards and principles contained in this Policy. Such assistance may relate to the establishment or adjustment of policies, the delivery of training or putting in place technical and organizational measures.

PARTNERSHIP TERMINATION

7.7. After termination of a partnership, all personal data collected in the performance of the partnership would be returned to the Group. Partnership agreements may provide for exceptions, in particular where there are legitimate reasons to do so, namely consent of the data subjects.

8. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

GENERAL CONDITIONS

8.1. The Group may disclose personal information to *inter alia* our associates and service providers, for legitimate business purposes, in accordance with applicable law and subject to applicable professional and regulatory requirements regarding confidentiality.

8.2. In addition, we may disclose personal information –

a) if required by law;
b) legal and regulatory authorities, upon request, or for the purposes of reporting any actual or suspected breach of applicable law or regulation;
c) third party Operators (including, but not limited to, data processors such as providers of data hosting services and document review technology and services), located anywhere in the world, subject to clauses 6.21 and 6.22.
d) where it is necessary for the purposes of, or in connection with, actual or threatened legal proceedings or establishment, exercise or defence of legal rights;
e) to any relevant party for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including, but not limited to, safeguarding against, and then prevention of threats to public security;
f) to any relevant third party acquirer(s), in the event that we sell or transfer all or any portion of our business or assets (including, but not limited to, in the event of a reorganization, dissolution or liquidation); and
g) to any relevant third party provider, where our website uses third party advertising, plugins or content.

8.3. The Group may only transfer personal data to third parties on condition that the third party affords a level of data protection the same or comparable to this Policy.

8.4. Given the potential data protection risks involved in transfers to third parties, the Group needs to pay particular attention to the following basic principles of this Policy:

a) Transfer is based on one or more legitimate bases;
b) Transfer is for one or more specific and legitimate purpose(s);
c) The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred;
d) The data subject has been informed, either at the time of collection in accordance with clauses 6.1 to 6.5, or subsequently, about the transfer of his/her personal data, unless one or more of the restrictions as described aboves;
e) The third party respects the confidentiality of personal data transferred to them by the Group. Whether or not a data transfer agreement has been signed between the Group and the third party, the Group must seek written agreement from the third party that the personal data will be kept confidential at all times. In order to ensure and respect confidentiality, personal data must be filed and stored in a way that is accessible only to authorized personnel and transferred only through the use of protected means of communication;
f) The third party maintains a high level of data security that protects personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to it.

8.5. In addition, the Group needs to ensure that transferring personal data does not negatively impact the safety and security of the Group's personnel and/or personnel of Implementing Partners; and/or

8.6. Before agreeing to transfer personal data to a third party, the Group needs to assess the level of data protection afforded by the third party. As part of this assessment, the data controller should assess, inter alia, the applicable laws and regulations, internal statutes and policies of the third party, specific contractual obligations or undertakings to respect specific data protection frameworks, their effective implementation as well as the technical and organizational means of data security put in place.

8.7. Pursuant to clauses 6.32 to 6.36, the data controller may need to carry out a DPIA.

DATA TRANSFER AGREEMENTS

8.8. Unless there are satisfactory reasons not to do so, prior to transferring personal data to a third party, the data controller should seek to sign a data transfer agreement, or, as appropriate, incorporate data protection clauses within broader agreements, particularly where transfers of personal data are likely to be large, repeated, or structural, i.e. where the same type(s) of data is shared with the same third party for the same purpose over a certain period of time.

8.9. Data transfer agreements should, *inter alia*:

a) (address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place;
b) require the third party to undertake that its data protection and data security measures are in
c) compliance with this Policy; and
d) stipulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement.

8.10. The officer and the legal & compliance department are to review and clear all data transfer agreements. Copies of final agreements are to be stored on Sharepoint.

9. ACCOUNTABILITY AND SUPERVISION

9.1. The Group's accountability and supervision structure referred will consist of the following key actors:
a) An officer (and deputy officers if necessary);
b) Data controllers in each department.

DATA PROTECTION OFFICER

9.2. The Group will appoint an officer, whose tasks will include:

a) Providing advice, support and training on data protection and this Policy;
b) Maintaining inventories of information provided by data controllers and data protection focal points, including data transfer agreements, specific instances of data sharing by the Group with third parties, DPIA's, data breach notifications and complaints by data subjects;
c) Actively encouraging data controllers and other relevant actors to undertake measures aimed at compliance with this Policy;
d) Monitoring and reporting on compliance with this Policy;
e) Liaising with the Legal and Compliance and Corporate Governance Department as necessary under this Policy.

DATA CONTROLLER

9.3. The data controller is responsible for establishing and overseeing the processing of personal data under his or her area of responsibility. He or she therefore also bears the main responsibility for compliance with the Policy.

9.4. The data controller, assisted by the officer, is to implement this policy by, *inter alia*:

a) Determining the applicable legitimate basis for and the specific and legitimate purposes of data processing;
b) Ensuring the implementation of organizational and security measures as well as assessing data security of third parties;
c) Establishing internal procedures, for example in the form of Data Protection Standard Operating Procedures, covering all relevant aspects of this Policy, in particular regarding the respect for the rights of the data subject and measures aimed at ensuring data confidentiality and security;
d) Ensuring that data protection and data security aspects are adequately included in Implementing Partner agreements;
e) Negotiating and concluding data transfer agreements with third parties as required or appropriate.

9.5. As necessary, the data controller should seek the advice of the officer concerning queries with regard to the application and interpretation of this policy.

10. CHANGES TO THIS POLICY

10.1. The Group may make amendments to this policy at any time without notice, so please ensure you view the latest version.

ANNEXURE 1: OWNERSHIP, APPROVAL & REVISION HISTORY

POLICY OWNER

The Data Protection Policy is owned by the Compliance Department who also maintains the document (as needed) in consultation with other relevant departments within the Group.

POLICY APPROVAL

The policy document was reviewed and approved by the by means of a round-robin resolution passed on the 24th of July 2024 by the Board of Prime Financial Services, the holding company of the Prime Investments Group, for distribution and implementation within the Group.

POLICY REVISION

Detailed below is a list of policy versions and the changes/amendments/additions made to the policy with each new version:

DATE	VERSION	CHANGES
May 2021	1.00	- Policy established
May 2023	1.01	- Format amendments.
June 2025	1.02	- Definitions have been added and amended in line with the Amended Regulations. - Email address for Information related queries or requests has been updated.