



PRIVACY POLICY

Declaring and documenting Fedgroup's commitment to the protection of privacy and personal information

Effective Date:	1 March 2021
Policy owner:	Audit and Risk and Compliance Committee
Prepared by:	Phumzile Nkabinde
Reviewed by:	Lelani Zaayman
Approved by:	All group entity boards
Entitles:	Relating to all entities in the Fedgroup Financial Holdings Proprietary Limited group of companies.
Committees	Audit and Risk Committee


Revision version	Date	Description of changes	Requested by
01		First implementation	LT
02	01/03 2021	Updated contact details	LT
03	31/05/ 2023	Review and update following internal changes	LvdM
04	24/05/ 2023	Review and update following internal changes	LvdM
05	28/05/2025	Review and update following internal changes	PN
06	31/08/2025	Review and update	PN
07	28/11/2025	Review and update	PN

CONTENTS

1. PREAMBLE.....	3
2. APPLICATION.....	3
3. GOVERNANCE.....	3
4. DEFINITIONS.....	3
5. LAWFUL PROCESSING OF PERSONAL INFORMATION.....	3
6. ACCOUNTABILITY.....	3
7. PROCESSING LIMITATION.....	4
8. PURPOSE SPECIFICATION.....	5
9. FURTHER PROCESSING LIMITATION.....	6
10. INFORMATION QUALITY.....	7
11. OPENNESS.....	7
12. SECURITY SAFEGUARDS.....	8
13. DATA SUBJECT PARTICIPATION.....	9
14. PROCESSING OF SPECIAL PERSONAL INFORMATION.....	10
15. PROCESSING OF PERSONAL INFORMATION OF CHILDREN.....	13
16. RIGHTS OF DATA SUBJECTS.....	14
17. TRANSBORDER INFORMATION TRANSFER.....	14
18. INFORMATION OFFICER.....	14
19. COMMITMENT TO COMPLIANCE.....	15
20. CONSEQUENCES OF NON-COMPLIANCE.....	15
21. PENALTIES.....	15
22. TRAINING.....	16
23. POLICY REVIEW.....	16
ANNEXURE 1: GENERAL INFORMATION.....	17
ANNEXURE 2: PRIVACY POLICY INFORMATION DOC.....	20


Fedgroup recognises the value as well as the risks associated with the regulatory requirements pertaining to its activities. This Privacy Policy has been approved by the Board of Directors of Fedgroup who have duly authorised the signatories to this document.

Signed on behalf of the Board:

Signed by:

1F0A70A3A1A744A...

Authorised Signatory
25 February 2026

Date

Signed by:

98128F038042416...

Authorised Signatory
05 March 2026

Date

1. PREAMBLE

The purpose of this Privacy Policy is to formally document and declare Fedgroup's commitment to respecting and protecting the privacy of our customers, keeping any information we have in our possession safe and confidential, and adhering to the requirements and regulations of the Protection of Personal Information Act.

2. APPLICATION

This Privacy Policy is applicable to Fedgroup Financial Holdings Group as a designated controlling company of the insurance group including its subsidiaries, collectively referred to as "Fedgroup".

3. GOVERNANCE

Within the governance structures of Fedgroup, this Privacy Policy is owned, and its administration overseen, by the Audit, Risk and Compliance Committee, who shall include suitable agenda items (standing and otherwise) to attend to the matters assigned to the Committee herein.

4. DEFINITIONS

Please refer to the Definitions section in the Governance Handbook

5. LAWFUL PROCESSING OF PERSONAL INFORMATION

The 8 conditions for the lawful processing of personal information are:

- i. Accountability
- ii. Processing limitation
- iii. Purpose specification
- iv. Further processing limitation
- v. Information quality
- vi. Openness
- vii. Security safeguards
- viii. Data subject participation

6. ACCOUNTABILITY

Fedgroup as a responsible party will not process any personal information in an unlawful manner or in contravention of POPIA.

7. PROCESSING LIMITATION

- 7.1. Fedgroup will ensure
- i. Lawfulness of processing
 - ii. Minimality
 - iii. Consent, justification, and objection
 - iv. Collection directly from the data subject

Lawfulness of processing

- 7.2. Fedgroup will only process personal information lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

Minimality

- 7.3. Fedgroup will only process personal information if, given the purpose for which it is processed, it is adequate, relevant, and not excessive.

Consent, justification, and objection

- 7.4. Fedgroup will only process personal information if,
- i. the data subject or a competent person where the data subject is a child consent to the processing.
 - ii. processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party.
 - iii. processing complies with an obligation imposed by law on the responsible party.
 - iv. processing protects a legitimate interest of the data subject.
 - v. processing is necessary for the proper performance of a public law duty by a public body; or
 - vi. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.
- 7.5. Fedgroup bears the burden of proof for the data subject's or competent person's consent.
- 7.6. The data subject or competent person may withdraw his, or her or its consent at any time, provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information will not be affected.
- 7.7. A data subject may object, at any time, to the processing of personal information in the prescribed manner, on reasonable grounds relating to his, her, or its particular situation, unless legislation provides for such processing; or for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.
- 7.8. If a data subject has objected to the processing of personal information Fedgroup will no longer process the personal information.

Collection directly from data subject

- 7.9. Fedgroup will at all times collect personal information directly from the data subject except if
- i. the information is contained in or derived from a public record or has deliberately been made public by the data subject.

- ii. the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source.
- iii. collection of the information from another source would not prejudice a legitimate interest of the data subject.
- iv. collection of the information from another source is necessary to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997); for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; in the interests of national security; or to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;
- v. compliance would prejudice a lawful purpose of the collection; or
- vi. compliance is not reasonably practicable in the circumstances of the particular case.

8. PURPOSE SPECIFICATION

8.1. Fedgroup will only collect and retain personal information for a specific purpose.

Collection for specific purpose

- 8.2. Fedgroup will only collect personal information for a specific explicitly defined and lawful purpose related to a function or activity within Fedgroup.
- 8.3. Fedgroup will ensure that the data subject is aware of the purpose of the collection of the information unless the collection is exempt from the notification requirement as further detailed in 11.2 below.

Retention and restriction of records

- 8.4. Fedgroup will not retain records of personal information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—
- i. retention of the record is required or authorised by law.
 - ii. the responsible party reasonably requires the record for lawful purposes related to its functions or activities.
 - iii. retention of the record is required by a contract between the parties thereto; or
 - iv. the data subject or a competent person where the data subject is a child has consented to the retention of the record.
- 8.5. Fedgroup will retain records of personal information for periods in excess of those contemplated above for historical, statistical or research purposes if subject to the establishment of appropriate safeguards against the records being used for any other purposes.
- 8.6. If Fedgroup used a record of personal information of a data subject to make a decision about the data subject, Fedgroup will retain the record for such period as may be required or prescribed by law or a code of conduct; or if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.
- 8.7. Fedgroup will destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after Fedgroup is no longer authorised to retain the record.
- 8.8. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

- 8.9. Fedgroup will restrict processing of personal information if—
- iv. its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information.
 - v. the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it must be maintained for purposes of proof.
 - vi. the processing is unlawful, and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
 - vii. the data subject requests to transmit the personal data into another automated processing system.
- 8.10. Restricted personal information referred to above may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.
- 8.11. Where processing of personal information is restricted Fedgroup will inform the data subject before lifting the restriction on processing.

9. FURTHER PROCESSING LIMITATION

- 9.1. Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.
- 9.2. To assess whether further processing is compatible with the purpose of collection, Fedgroup take account of—
- i. the relationship between the purpose of the intended further processing and the purpose for which the information has been collected.
 - ii. the nature of the information concerned.
 - iii. the consequences of the intended further processing for the data subject.
 - iii. the manner in which the information has been collected; and
 - iv. any contractual rights and obligations between the parties.
- 9.3. The further processing of personal information is not incompatible with the purpose of collection if—
- i. the data subject or a competent person where the data subject is a child has consented to the further processing of the information.
 - ii. the information is available in or derived from a public record or has deliberately been made public by the data subject.
 - iii. further processing is necessary— to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution, and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997); (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or in the interests of national security;
 - iv. the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to— public health or public safety, or the life or health of the data subject or another individual.
 - v. the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or
 - vi. the further processing of the information is in accordance with an exemption granted in terms of POPIA.

10. INFORMATION QUALITY

Fedgroup will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading, and updated where necessary while having regard to the purpose for which personal information is collected or further processed.

11. OPENNESS

Documentation

11.1. Fedgroup will maintain the documentation of all processing operations under its responsibility as required in terms of POPIA

Notification to data subject when collecting personal information

11.2. Fedgroup will, when collecting personal information, take reasonably practicable steps to ensure that the data subject is aware of—

11.3.

- i. the information being collected and where the information is not collected from the data subject, the source from which it is collected.
- ii. the name and address of the responsible party.
- iii. the purpose for which the information is being collected.
- iv. whether or not the supply of the information by that data subject is voluntary or mandatory.
- v. the consequences of failure to provide the information.
- vi. any particular law authorising or requiring the collection of the information.
- vii. the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.
- viii. any further information such as the recipient or category of recipients of the information, nature or category of the information, existence of the right of access to and the right to rectify the information collected existence of the right to object to the processing of personal information and right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

11.4. The reasonable steps referred to above will be taken—

- i. if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or
- ii. in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

11.5. It is not necessary for Fedgroup to comply with the above notification requirement if—

- i. the data subject or a competent person where the data subject is a child has provided consent for the non-compliance.
- ii. non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act.
- iii. non-compliance is necessary to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences, to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997),

- iv. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or in the interests of national security;
- v. compliance would prejudice a lawful purpose of the collection.
- vi. compliance is not reasonably practicable in the circumstances of the particular case; or
- vii. the information will not be used in a form in which the data subject may be identified; or be used for historical, statistical or research purposes.

12. SECURITY SAFEGUARDS

Security measures on integrity and confidentiality of personal information

- 12.1. Fedgroup will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
- i. loss of, damage to or unauthorised destruction of personal information; and
 - ii. unlawful access to or processing of personal information.
- 12.2. In order to give effect to the above), Fedgroup will take reasonable measures to—
- i. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control.
 - ii. establish and maintain appropriate safeguards against the risks identified.
 - iii. regularly verify that the safeguards are effectively implemented; and
 - iv. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- 12.3. Fedgroup will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations. Please refer to the Cyber Security Policy for further information.

Information processed by operator or person acting under authority

- 12.4. An operator or anyone processing personal information on behalf of Fedgroup or an operator, must process such information only with the knowledge or authorisation of Fedgroup and treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

Security measures regarding information processed by the operator

- 12.5. Fedgroup will enter into a written contract with any operator, to ensure that the operator which processes personal information on behalf of Fedgroup establishes and maintains the security measures referred to above and require that the operator notifies Fedgroup immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person

Notification of security compromises

- 12.6. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, Fedgroup will notify—
- i. the Regulator; and
 - ii. subject to the below, the data subject, unless the identity of such data subject cannot be established.

- 12.7. The notification referred to above must be made as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of Fedgroup's information systems.
- 12.8. Fedgroup may only delay notification of the data subject if a public body responsible for the prevention, detection, or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.
- 12.9. The notification to a data subject referred to above must be in writing and communicated to the data subject in at least one of the following ways:
- i. mailed to the data subject's last known physical or postal address.
 - ii. sent by e-mail to the data subject's last known e-mail address.
 - iii. placed in a prominent position on the website of the responsible party.
 - iv. published in the news media; or
 - v. as may be directed by the Regulator.
- 12.10. The notification referred to above must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—
- i. a description of the possible consequences of the security compromise.
 - ii. a description of the measures that the responsible party intends to take or has taken to address the security compromise.
 - iii. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
 - iv. if known to Fedgroup, the identity of the unauthorised person who may have accessed or acquired the personal information.
- 12.11. The Regulator may direct Fedgroup to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

13. DATA SUBJECT PARTICIPATION

Access to personal information

- 13.1. A data subject, having provided adequate proof of identity, has the right to— (a)
- i. request Fedgroup to confirm, free of charge, whether or not we hold personal information about the data subject; and
 - ii. request from Fedgroup the record or a description of the personal information about the data subject held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information within a reasonable time at a prescribed fee, if any; in a reasonable manner and format; and in a form that is generally understandable.
- 13.2. If in response to a request in terms of the above, personal information is communicated to a data subject, the data subject must be advised of the right to request the correction of information.
- 13.3. If a data subject is required to pay a fee for services provided to the data subject Fedgroup—
- i. must give the applicant a written estimate of the fee before providing the services; and
 - ii. may require the applicant to pay a deposit for all or part of the fee. (

- 13.4. Fedgroup may or must refuse, as the case may be, to disclose any information requested to which the grounds for refusal of access to records set out in the Promotion of Access to Information Act (PAIA) apply.
- 13.5. If a request for access to personal information is made to Fedgroup and part of that information may or must be refused, every other part must be disclosed.

Correction of personal information

- 13.6. A data subject may, in the prescribed manner, request Fedgroup to—
 - i. correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or
 - ii. destroy or delete a record of personal information about the data subject that Fedgroup is no longer authorised to retain.
- 13.7. On receipt of a request to correct information Fedgroup will as soon as reasonably practicable—
 - i. correct the information.
 - ii. destroy or delete the information.
 - iii. provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or
 - iv. where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
- 13.8. If Fedgroup has taken steps that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, Fedgroup must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.
- 13.9. Fedgroup will notify a data subject, who has made a correction request of the action taken as a result of the request.

Manner of access

- 13.10. The provisions of the PAIA apply to personal information requests made in terms of POPIA.

14. PROCESSING OF SPECIAL PERSONAL INFORMATION

Prohibition on processing of special personal information

- 14.1. Fedgroup may not, subject to the below, process personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject 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.

General authorisation concerning special personal information

- 14.2. The prohibition on processing of special personal information does not apply if the—
- i. processing is carried out with the consent of a data subject
 - ii. processing is necessary for the establishment, exercise, or defence of a right or obligation in law.
 - iii. processing is necessary to comply with an obligation of international public law.
 - iv. processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest, and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.
 - v. information has deliberately been made public by the data subject; or
 - vi. the provisions of POPIA with regards to the use of special personal information as further detailed below, as the case may be, were complied with.
- 14.3. The Regulator may authorise Fedgroup to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject and may impose reasonable conditions in respect of any authorisation granted.

Authorisation concerning data subject's religious or philosophical beliefs

- 14.4. The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, does not apply if the processing is carried out by—
- i. spiritual or religious organisations, or independent sections of those organisations if the information concerns data subjects belonging to those organisations; or it is necessary to achieve their aims and principles.
 - ii. institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or
 - iii. other institutions.

Provided that the processing is necessary to protect the spiritual welfare of the data subjects unless they have indicated that they object to the processing.

- 14.5. The prohibition does not apply to the processing of personal information concerning the religion or philosophy of life of family members of the data subjects if the association concerned maintains regular contact with those family members in connection with its aims; and the family members have not objected in writing to the processing.
- 14.6. Personal information concerning a data subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

Authorisation concerning data subject's race or ethnic origin

- 14.7. The prohibition on processing personal information concerning a data subject's race or ethnic origin, does not apply if the processing is carried out to identify data subjects and only when this is essential for that purpose; and if it complies with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Authorisation concerning data subject's trade union membership

14.8. The prohibition on processing personal information concerning a data subject's trade union membership does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs if such processing is necessary to achieve the aims of the trade union or trade union federation.

14.9. No personal information may be supplied to third parties without the consent of the data subject.

Authorisation concerning data subject's political persuasion

14.10. The prohibition on processing personal information concerning a data subject's political persuasion, does not apply to processing by or for an institution, founded on political principles, of the personal information of—

- i. its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or
- ii. a data subject if such processing is necessary for the purposes of forming a political party, participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party with the view to an election of the National Assembly or the provincial legislature, municipal elections or a referendum or campaigning for a political party or cause.

14.11. No personal information may be supplied to third parties without the consent of the data subject.

Authorisation concerning data subject's health or sex life

14.12. The prohibition on processing personal information concerning a data subject's health or sex life, does not apply to the processing by—

- i. medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned.
- ii. insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing; the performance of an insurance or medical scheme agreement; or the enforcement of any contractual rights and obligations.
- iii. schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life.
- iv. any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties.
- v. any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or
- vi. administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

14.13. The information may only be processed by Fedgroup subject to an obligation of confidentiality by virtue of office, employment, profession, or legal provision, or established by a written agreement between Fedgroup and the data subject.

- 14.14. If Fedgroup is permitted to process information concerning a data subject's health or sex life and is not subject to an obligation of confidentiality by virtue of office, profession, or legal provision, Fedgroup will still treat the information as confidential, unless required by law or in connection with any duties to communicate the information to other parties who are authorised to process such information.
- 14.15. The prohibition does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, with a view to the proper treatment or care of the data subject.
- 14.16. Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless a serious medical interest prevails; or the processing is necessary for historical, statistical or research activity.

Authorisation concerning data subject's criminal behaviour or biometric information

- 14.17. The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.
- 14.18. The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

15. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

Prohibition on processing personal information of children

- 15.1. As a general rule - Fedgroup may not process personal information concerning a child.

General authorisation concerning personal information of children

- 15.2. The prohibition on processing personal information of children, does not apply if the processing is—
- i. carried out with the prior consent of a competent person;
 - ii. necessary for the establishment, exercise, or defence of a right or obligation in law;
 - iii. necessary to comply with an obligation of international public law;
 - iv. for historical, statistical or research purposes to the extent that the purpose serves a public interest, and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
 - v. of personal information which has deliberately been made public by the child with the consent of a competent person.
- 15.3. The Regulator may authorise Fedgroup to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.
- 15.4. The Regulator may impose reasonable conditions in respect of any authorisation granted including conditions with regard to how a Fedgroup must—
- i. upon request of a competent person provide a reasonable means for that person to review the personal information processed; and refuse to permit its further processing.
 - ii. provide notice regarding the nature of the personal information of children that is processed, how such information is processed, and regarding any further processing practices.

- iii. refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and
- iv. establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

16. RIGHTS OF DATA SUBJECTS

- 16.1. 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 including the right—
- i. to be notified that personal information about him, her or it is being collected; or his, her or its personal information has been accessed or acquired by an unauthorised person
 - ii. to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information
 - iii. to request, where necessary, the correction, destruction, or deletion of his, her or its personal information
 - iv. to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information
 - v. to object to the processing of his, her or its personal information at any time for purposes of direct marketing or not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications
 - vi. not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person
 - vii. to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator and
 - viii. to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

17. TRANSBORDER INFORMATION TRANSFER

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

18. INFORMATION OFFICER

- 18.1. Fedgroup has appointed Information Officers as further detailed in Annexure 1 to perform the duties and responsibilities as set out in POPIA.
- 18.2. The information officer's responsibilities include—
 - i. the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information.
 - ii. dealing with requests made to the body pursuant to POPIA
 - iii. working with the Regulator in relation to investigations
 - iv. otherwise ensuring compliance by Fedgroup with the provisions of POPIA; and
 - v. as may be prescribed.
- 18.3. Information Officers will only take up their duties after Fedgroup registered them with the Information Regulator.

19. COMMITMENT TO COMPLIANCE

- 19.1. Fedgroup have developed, documented, and will maintain and implement this policy to ensure the protection of the personal information of all customers.
- 19.2. Fedgroup will make documentation describing this policy available to each of its employees involved in transactions to which POPIA applies.
- 19.3. Fedgroup will, on request, make a copy of this policy available to the Information regulator; or any other supervisory body which performs regulatory or supervisory functions.
- 19.4. The Boards of Directors of Fedgroup will ensure compliance with the provisions of POPIA and this policy.
- 19.5. The GRC Function of Fedgroup will assist the Boards of Directors in discharging their obligations under POPIA and the policy and Fedgroup will assign persons with sufficient competence and seniority to ensure the effectiveness of the policy and compliance by the employees of Fedgroup with the provisions of POPIA.
- 19.6. Please refer to Annexure 1 for further detail on the Information Officers and Information Regulator and complaint process.
- 19.7. Fedgroup will ensure the continued registration with the Information Regulator (IR) as prescribed.
- 19.8. Fedgroup will notify the IR in writing of any changes to the particulars furnished within the prescribed timelines.

20. CONSEQUENCES OF NON-COMPLIANCE

- 20.1. Any failure by an employee to comply with the requirements of POPIA or this Privacy Policy shall result in the employee being subject to disciplinary action and possible dismissal.

21. PENALTIES

- 21.1. A person convicted of an offence in terms of POPIA, is liable, in the case of a contravention of section 100 (Obstruction of Regulator), 103(1) (Failure to comply with enforcement or information notice in terms of section 95), 104(2) (Offences by witnesses), 105(1) (Unlawful acts by responsible party in connection with account number), 106(1), (3) or (4) (Unlawful acts by third parties in connection with

account number) to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment.

- 21.2. A person convicted of an offence in terms of POPIA, is liable, in the case of a contravention of section 59 (failure to notify processing subject), 101 (breach of confidentiality), 102 (obstruction of execution warrant), 103(2) (Failure to comply with enforcement or information notice in terms of section 90) or 104(1) (Offences by witnesses), a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

22. TRAINING

- 22.1 Fedgroup will provide ongoing training to its employees to enable their compliance with the provisions of POPIA and the Privacy Policy. All employees of Fedgroup whether permanent or part-time, will receive proportionate training necessary to their job function.

23. POLICY REVIEW

- 23.1. This Policy will undergo a review on an annual basis to ensure that the policy and procedures remain relevant to Fedgroup's operations and the achievement of the purpose of the policy.
- 23.2. Any relevant ad-hoc event within the scope of this policy e.g., change in regulation or operational requirements, identification of an inadequacy of any element of this policy etc. will prompt a review of this policy as and when required.

ANNEXURE 1: GENERAL INFORMATION

1.1 Every employee of Fedgroup is responsible to ensure compliance with this policy, however the Board and Senior Management is ultimately accountable to ensure compliance with POPIA and other applicable legislation. Please refer to the Governance Framework for further detail on the Board and senior management.

1.2. The Information Officer details are as follows:

Entity	Information Officer	Deputy Information Officer
Fedgroup Financial Holdings	Grant Field grantfi@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Thobile Mlambo thobilem@fedgroup.co.za
Fedgroup Life Limited	Michael Field michaelf@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Natasha Ndyamba natashand@fedgroup.co.za Fiona Klose fionak@fedgroup.co.za
Fedgroup Trust Administrators	Michael Field michaelf@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Phumzile Nkabinde PhumzileN@fedgroup.co.za Fiona Klose fionak@fedgroup.co.za
Fedgroup Financial Services	Paul Counihan paulc@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Phumzile Nkabinde PhumzileN@fedgroup.co.za Iris Marais irism@fedgroup.co.za
Fedgroup Employee Benefits	Michael Field michaelf@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Zanele Mahlangu zanelem@fedgroup.co.za Fiona Klose fionak@fedgroup.co.za
Fedgroup Asset Management	Paul Counihan paulc@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Natasha Ndyamba natashand@fedgroup.co.za Iris Marais irism@fedgroup.co.za
Fedgroup Participation Bond Managers	Stef Valenti stefv@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Thobile Mlambo thobilem@fedgroup.co.za Jason Green jasong@fedgroup.co.za Iris Marais irism@fedgroup.co.za

		Yoni Bender Yonib@fedgroup.co.za
Fedgroup Management	Paul Counihan paulc@fedgroup.co.za	Paul Green paulg@fedgroup.co.za Zanele Mahlangu zanelem@fedgroup.co.za Iris Marais irism@fedgroup.co.za

1.3. DUTIES OF THE INFORMATION OFFICER

Section 55(1) of POPIA sets out the duties and responsibilities of an Information Officer which includes the following: -

- 1.3.1. the encouragement of compliance by Fedgroup with the conditions for the lawful processing of personal information. For example, an Information Officer may develop a policy on how employees should implement the eight (8) conditions for the lawful processing of personal information.
- 1.3.2. dealing with requests made to Fedgroup pursuant to POPIA. For example, an Information Officer will be expected to render such reasonable assistance, free of charge, as is necessary to enable the requester or data subject to comply with the prescribed process for submitting a request in terms of section 18 of PAIA and section 24 of POPIA. If a requester or data subject has made any request that does not comply with the requirements of PAIA or POPIA, the Information Officer may not refuse the request because of that noncompliance, unless the Information Officer has-
 - a) notified the data subject or requester of his/her intention to refuse the request and stated in the notice, the reasons for the contemplated refusal, as well as his/her availability to assist that requester or data subject to remove the grounds for refusal.
 - b) given the requester or data subject a reasonable opportunity to seek such assistance.
 - c) as far as reasonably possible, furnished the requester or data subject with any information that would assist the making of the request in the prescribed form; and
 - d) given the requester a reasonable opportunity to confirm the request or alter it to comply with section 18 of PAIA or 24 of POPIA.
- 1.3.3. working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA. For example, the responsible party must obtain prior authorisation from the Regulator pertaining to the following
 - a) processing of any unique identifiers of data subjects i. for a purpose other than the one for which the identifier was specifically intended at collection; and ii. with the aim of linking the information together with information processed by other responsible parties.
 - b) processing of information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties.
 - c) processing of information for the purposes of credit reporting; and
 - d) transfer of special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.
- 1.3.4. pending the authorisation or completion of investigation by the Regulator, or until such time the responsible party receives a notice that a more detailed investigation will not be conducted, the responsible party is prohibited from carrying out information processing. This means that processing that falls under paragraph 1.3.1 above is suspended pending the authorisation from the Regulator. Failure to notify the Regulator of the processing listed above is an offence and upon conviction, the

responsible party will be liable to a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

1.3.7. otherwise ensuring compliance by Fedgroup with the provisions of POPIA. For example, POPIA prescribes eight (8) conditions for the lawful processing of personal information by or for a responsible party and it is the responsibility of an Information Officer to ensure compliance with those conditions.

1.3.8. The additional duties and responsibilities of the Information Officers, in terms of regulation 4 of POPIA, are to ensure that

- a) a compliance framework is developed, implemented, monitored and maintained.
- b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
- c) a manual is developed, monitored, maintained, and made available as prescribed in sections 14 and 51 of PAIA, as amended.
- d) internal measures are developed together with adequate systems to process requests for information or access thereto.
- e) internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator; and
- f) upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time.

1.3.9. The Regulator may, annually, request an Information Officer of a private body, in terms of section 83 (4) of PAIA, to furnish to the Regulator with information about requests for access to records of that body.

1.3.10. In the case of health records, if the Information Officer is of the opinion that the disclosure of the record to the relevant person would be likely to cause serious harm to their physical or mental health, or well-being, the Information Officer may only give access to the record if the requester proves to the satisfaction of the information officer that adequate provision is made for such counselling or arrangements as are reasonably practicable before, during or after the disclosure of the record to limit, alleviate or avoid such harm to the relevant person.

1.3.11. Registration of Information Officers¹⁵ with the Regulator is not only the prerequisite for an Information Officer to take up their duties in terms of POPIA but is a compulsory requirement.

1.3.12. The Information Officers of public bodies and heads of private bodies under PAIA will have to register to perform their duties and responsibilities in terms of POPIA. It is a duty of the responsible party to ensure that the Information Officer is registered with the Regulator.

1.4. The Information Regulator's contact details are as follows:

Contact - Information Regulator (info regulator.org.za)

ANNEXURE 2: PRIVACY POLICY INFORMATION DOC

Introduction

We respect your privacy and take the protection of **personal information** very seriously. The purpose of this policy is to describe the way that we collect, store, use, and protect information that can be associated with you or another specific natural or juristic person and can be used to identify you or that person.

The purpose of this policy is to describe the way that we handle your personal information.

This policy applies to you if you are:

- a visitor to our website.
- use our mobile App; or
- a customer who has ordered or requested the products or services that we provide.

Your rights under this Privacy Policy

You have the right to have your personal information processed lawfully. Your rights include the right:

- to be notified that your personal information is being collected or that your personal information has been accessed or acquired by an unauthorised person e.g., where a hacker may have compromised our computer system.
- to find out whether we hold your personal information and to request access to your personal information.
- to request us, where necessary, to correct, destroy or delete your personal information.
- to object, on reasonable grounds, to the processing of your personal information.
- to object to the processing of your personal information for purposes of direct marketing, including by way of unsolicited communications.
- to submit a complaint to the Regulator if you believe that there has been interference with the protection of your personal information, or if you believe that an independent adjudicator who may be resolving your complaint against us, has not decided the matter correctly; and
- to institute civil proceedings against us if you believe that we have interfered with the protection of your personal information.

Personal Information

The personal information includes:

- certain information that we collect automatically when you visit our website or mobile App.
- certain information collected on registration (see below).
- certain information collected on submission; and
- optional information that you provide to us voluntarily (see below); **but excludes:**
- information that has been made anonymous so that it does not identify a specific person.
- permanently de-identified information that does not relate or cannot be traced back to you specifically;
- non-personal statistical information collected and compiled by us; and
- information that you have provided voluntarily in an open, public environment or forum including any blog, chat room, community, classifieds, or discussion board (because the information has been disclosed in a public forum, it is no longer confidential and does not constitute personal information subject to protection under this policy).

We will not intentionally collect and process the personal information of a child unless we have the permission of a competent or authorised person.

Personal information includes information we collect (i) automatically when you visit our website or use our mobile App, (ii) on registration, (iii) on submission, and (iv) from you voluntarily. It excludes (i) anonymous, (ii) de-identified, (iii) non-personal statistical, and (iv) public information.

Common examples

Common examples of the types of personal information which we may collect, and process include your:

- **identifying information** – such as your name, date of birth, or identification number of any kind.
- **contact information** – such as your phone number or email address.
- **address information** – such as your physical or postal address; or
- **demographic information** – such as your gender or marital status.

Sensitive personal information

Depending on the products or services that you require, we may also collect sensitive personal information including your:

- **financial information** – such as your bank account details.
- **sensitive demographic information** – such as your race or ethnicity.
- **medical information** – such as information about your physical or mental health.
- **criminal information** – such as information about your commission or alleged commission of any offence or about any related legal proceedings.
- **employment information** – including your membership of a trade union; and

Acceptance

It is important that you read, understand, and accept our Terms of Service if you would like to use our services. You must accept all the terms of this policy when you order our products or request our services. If you do not agree with anything in this policy, then you may not order our products or request our services. You may not order our products or request our services if you do not accept this policy.

Legal capacity

You may not access our website or mobile App or order our products or request our services if you are younger than 18 years old or do not have legal capacity to conclude legally binding contracts.

Deemed acceptance

By accepting this policy, you are deemed to have read, understood, accepted, and agreed to be bound by all of its terms.

Your obligations

You may only send us your personal information or the information of another data subject where you have their permission to do so.

Changes

We may change the terms of this policy at any time by updating this web page. Please ensure that you visit our website and regularly read this Privacy Policy. Although we do not promise to do so, we may give you notice of any changes we think are important.

If you do not agree with the changes, then you must stop using the website or mobile App and our products or services. If you continue to use the website, mobile App or our products or services following

notification of a change to the terms, the changed terms will apply to you, and you will be deemed to have accepted those updated terms.

Collection

On registration

We collect certain information on registration when you register on our website or mobile App.

Once you register on our website or mobile App, you will no longer be anonymous to us. You will provide us with certain personal information when you register. This personal information will include:

- your name and surname.
- your identity numbers.
- your email address.
- your telephone numbers.
- your company name, company registration number, and VAT number.
- your postal address or street address; and
- your username and password.

We will use this personal information to fulfil your account and provide additional services and information to you as we reasonably think appropriate, and for any other purposes set out in this policy.

On order or request

We collect certain information when you order our products or request our services from us.

When you order our products or request our services from us, you may be asked to provide us with additional information on a voluntary basis (**products or services information**).

Cookies

We may collect certain information from your web browser, including your Internet usage information when you visit our website.

We may place small text files called 'cookies' on your device when you visit our website. These files do not contain personal information, but they do contain a personal identifier allowing us to associate your personal information with a certain device. These files serve a number of useful purposes for you, including:

- tailoring our website's functionality to you personally by letting us remember your preferences.
- improving how our website performs.
- allowing third parties to provide services to our website; and

Your internet browser generally accepts cookies automatically, but you can often change this setting to stop accepting them. You can also delete cookies manually. However, no longer accepting cookies or deleting them will prevent you from accessing certain aspects of our website where cookies are necessary. Many websites use cookies, and you can find out more about this in our [Cookie Policy](#).

Optional details

You may also provide additional information to us on a voluntary basis (optional information). This includes content or products that you decide to upload or download from our website or mobile App or when you enter competitions, take advantage of promotions, respond to surveys, order certain additional products or services, or otherwise use the optional features and functionality available.

Recording calls

We may monitor and record any telephone calls that you make to us unless you specifically request us not to.

Purpose for collection

We may use any of your personal information that you provide to us for the purposes that you indicated when you agreed to provide it to us.

We may use or process any products or services information, or optional information that you provide to us for the purposes that you indicated when you agreed to provide it to us. Processing includes gathering your personal information, disclosing it, and combining it with other personal information. We generally collect and process your personal information for various purposes, including:

- **products or services purposes** – such as collecting applications or requests for and providing our products or services.
 - **marketing purposes** – such as pursuing lawful related marketing activities.
 - **business purposes** – such as internal audit, accounting, business planning, and joint ventures, disposals of business, or other proposed and actual transactions; and
 - **legal purposes** – such as handling claims, complying with regulations, or pursuing good governance.
- We may use your usage information for the purposes described above and to:
- remember your information so that you will not have to re-enter it during your visit or the next time you access the website or mobile App.
 - monitor website and mobile App usage metrics such as total number of visitors and pages accessed; and
 - track your entries, submissions, and status in any promotions or other activities in connection with your usage of the website or mobile App.

Consent to collection

We will get your consent to collect your personal information in accordance with applicable law when you provide us with it.

You consent to the collection of your personal information in accordance with applicable law when you provide us with any registration information or optional information.

Use

Our obligations

We may use your information to send you administrative messages and email updates to you regarding the website or mobile App and for marketing purposes where lawful.

We may use your personal information to fulfil our obligations to you.

Messages and updates

We may send administrative messages and email updates to you about the products and services you subscribe to. In some cases, we may also send you primarily promotional messages. You can choose to optout of promotional messages and unsubscribe from email updates. We will not send you promotional messages unless you have chosen to opt-into them.

Disclosure Sharing

We may share your personal information with third parties for the purposes of fulfilling our obligations to you among other purposes.

We may share your personal information with:

- other divisions or companies within the group of companies to which we belong to provide joint content and services like registration, for transactions and customer support, to help detect and prevent potentially illegal acts and violations of our policies, and to guide decisions about our products, services, and communications (they will only use this information to send you marketing communications if you have requested their products or services).

- an affiliate, in which case we will seek to require the affiliates to honour this privacy policy.
- our products or services providers under contract who help provide certain products or services or help with parts of our business operations, including underwriting, fraud prevention, bill collection, marketing, technology services (our contracts dictate that these products or services providers only use your information in connection with the products or services they supply or services they perform for us and not for their own benefit).
- credit bureaus to report account information (where applicable), as permitted by law.
- banking partners as required by credit card association rules for inclusion on their list of terminated merchants (if you utilise the services to receive payments and you meet their criteria); and
- other third parties who provide us with relevant services where appropriate.
- We will ensure that your personal information is processed in a lawful manner and that the third parties or we do not infringe your privacy rights. If we ever outsource the processing of your personal information to a third-party operator, we will ensure that the operator processes and protects your personal information using reasonable technical and organisational measures that are equal to or better than ours.

Regulators

We may disclose your personal information as required by law or governmental audit.

We may disclose personal information to third parties if required for legal reasons.

Ombudsman

We may disclose your personal information to the Ombudsman if required.

Law enforcement

We may disclose personal information if required:

- by a subpoena or court order.
- to comply with any law.
- to protect the safety of any individual or the general public; and
- to prevent violation of our customer relationship terms.

No selling

We will not sell personal information. No personal information will be disclosed to anyone except as provided in this privacy policy.

Marketing purposes

We may disclose aggregate statistics (information about the customer population in general terms) to service providers or business partners.

Employees

We may need to disclose personal information to our employees that require the personal information to do their jobs. These include our responsible management, human resources, accounting, audit, compliance, information technology, or other personnel.

Security

Our website and services are hosted on a secure server and uses security measures to prevent interference by intruders.

We take the security of personal information very seriously and always do our best to comply with applicable data protection laws and to secure the integrity and confidentiality of your personal information

in our possession or under our control. We will do this by taking appropriate, reasonable technical and organisational measures to prevent loss of damage to or unauthorised destruction of your personal information, and unlawful access to or processing of your personal information. Our hosting company hosts our website and servers in a secure environment that uses a firewall and other advanced security measures to prevent interference or access from outside intruders. We authorise access to personal information only for those employees who require it to fulfil their job responsibilities. We implement disaster recovery procedures where appropriate.

Accurate and up to date

Please keep your personal information accurate and up to date by accessing your account online, emailing us, by phoning us.

We will try to keep the personal information we collect as accurate, complete, and up to date as is necessary for the purposes defined in this policy. From time to time, we may request you to update your personal information on the website, mobile App or through other channels. You can review or update any personal information that we hold on to you by accessing your account online, emailing us, or phoning us. Please note that in order to better protect you and safeguard your personal information, we take steps to verify your identity before granting you access to your account or making any corrections to your personal information.

Retention

We will only retain your personal information for as long as is necessary.

We will only retain your personal information for as long as it is necessary to fulfil the purposes explicitly set out in this policy, unless:

- retention of the record is required or authorised by law; or
- you have consented to the retention of the record.

During the period of retention, we will continue to abide by our non-disclosure obligations and will not share or sell your personal information.

We may retain your personal information in physical or electronic records at our discretion.

Transfer to another country

We will not transfer any personal information across a country border without your prior written consent.

We may not transfer your personal information outside the country in which it was collected to a foreign country without your permission.

Updating or removing

You may choose to correct or update the personal information you have submitted to us, by completing a Request for Correction or Deletion of Personal Information form in the relevant menu in the pages on our website or contacting us by phone or email.

You may choose to update or remove the personal information you have submitted to us.

Limitation

We are not responsible for, give no warranties, nor make any representations in respect of the privacy policies or practices of linked or any third-party websites.

Enquiries

If you have any questions or concerns arising from this privacy policy or the way in which we handle personal information, please contact us @ popia@fedgroup.co.za.

ANNEXURE 3: COOKIE POLICY

Introduction

Our Cookie Policy works alongside our Privacy Policy and aims to describe what cookies are, what we use them for, and how you can manage them during your visit to, or use of, our website.

This policy applies to Fedgroup Financial Holdings (Pty) Ltd., a licensed controlling company, and its subsidiaries (hereinafter "Fedgroup").

What are cookies?

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used to make websites work, or work more efficiently, as well as to provide information to the owners of the site. These files do not contain personal data, but they do contain a personal identifier allowing us to associate your personal data with a certain device. Many websites use cookies and you can find out more about them at www.aboutcookies.org or www.allaboutcookies.org.

Why do we use cookies?

These files (cookies) serve a number of useful purposes for you, including:

- granting you access to restricted content;
- tailoring our website's functionality to you personally by letting us remember your preferences, location or device type;
- improving how our website performs;
- understanding who our audience is so that we can provide content most relevant to you;
- allowing third parties to provide services to our website; and
- helping us deliver interest-based advertising where appropriate in compliance with the applicable laws.

Types of cookies we use

We use different types of cookies on our website. Some of these cookies are placed by us, while others are placed by our third-party plug-ins or suppliers. These cookies may be deleted from your device at different

times, such as at the end of your browsing session (when you leave the website) or after a pre-set amount of time, or they may stay on your device until you delete them.

We use the following types of cookies on our website:

Necessary cookies – these are cookies that allow our website to perform its essential functions. Without these cookies, some parts of our websites would stop working.

Preferences (Functional) cookies – these are cookies that remember who you are as a user of our website. We use them to remember any preferences you may have selected on our website, like saving your username and password or settings.

Statistics cookies – these are cookies that remember how you interacted with the website. We use them to help understand visitor behaviour and improve the site's performance and usability.

Marketing cookies – these are cookies used to deliver advertised content which is relevant to you and that can be used to measure the effectiveness of our campaigns.

Changing cookies

Your internet browser generally accepts cookies automatically, but you can often change this setting to stop accepting them. You can also delete cookies manually.

You can find out how to do this at www.digitaltrends.com/computing/how-to-delete-cookies. By clicking on the following link, you can also change your consent and preferences at any time.

What is the duration of the cookies we use?

In terms of duration, we may use two different types of cookies on our website:

Session Cookies: These cookies are temporary and last only for the duration of your web session and expire when you close your browser.

Persistent Cookies: These cookies remain on your computer, smart phone or tablet for a longer duration as it enables us to remember your login details for when you return to our website. These cookies last for a period of 1 (one) year.

Deleting cookies

Deleting or no longer accepting cookies may prevent you from accessing certain aspects of our website where cookies are necessary, or because the website forgot your preferences.

On our mobile App

Our mobile App uses technology called a webview to display online content. Cookies are stored within a webview like they are stored in a browser setting. Webview is similar to mobile browsers because it is unique per application and cannot share cookie information between Apps or the device's web browser.

Mobile Apps operate independently of each other. Each App functions as a standalone product and has an incredibly limited ability to access data from other Apps. Because of this, though cookies can store a user's preferences within an App, other Apps cannot access those preferences.

Updates and changes

We may occasionally make changes to the policy and will update the web page. Please ensure that you visit our website and regularly read this **Cookie Policy**. Although we do not promise to do so, we may give you notice of any changes we think are important.

APPENDIX 1: FORMS

- [FORM SCN1 – Security Compromises Notification – Fillable Form](#)
- Form 1: [Objection to the Processing of Personal Information](#)
- Form 2: [Request for Correction or Deletion of Personal Information or Destroying or Deletion of Record of Personal Information](#)
- Form 5: [Complaint Regarding Interference with the Protection of Personal Information/Complaint Regarding Determination of an Adjudicator](#)