First National Bank

First National Bank Ghana Internal Privacy Policy

28 July 2023

DOCUMENT CONTROL

Title	First National Bank Ghana Internal Privacy Policy		
Author	Group Compliance		
Document version	2		
Version date	TBC		
Approval	Committee for Approval:	Approval date:	Version for approval:
	Risk Committee	28 July 2023	2
Next Review Date	28 July 2025		

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE 4
2. DEFINITIONS 6
3. APPLICABILITY AND SCOPE 8
4. PRINCIPLES APPLICABLE TO THE HANDLING OF PI AND SPI 9
4.1.1. Privacy Principle 1: Accountability 9
4.1.2. Privacy Principle 2: Processing Limitation 9
4.1.3. Privacy Principle 3: Purpose Specification 12
4.1.4. Privacy Principle 4: Further Processing 12
4.1.5. Privacy Principle 5: Information Quality 13
4.1.6. Privacy Principle 6: Openness 13
4.1.7. Privacy Principle 7: Security Safeguards 13
4.1.8. Privacy Principle 8: Data Subject Participation 14
4.1.9. Privacy Principle 9: Cross Border Transfer of Personal Information 14
4.1.10. Privacy Principle 10: Third Party / Operator Management 15
5. GENERAL 15
6. OWNERSHIP AND REVIEW 15
ANNEXURE 1: SPECIFIC IN-COUNTRY REQUIREMENTS RELATING TO DATA SUBJECT RIGHTS 16

1. BACKGROUND AND PURPOSE

Confidentiality of information and the secure retention thereof are entrenched concepts in the financial world. How information is handled and protected has become an increasingly important concern in a global society. It is important to understand the significance and value of information as a business asset which enables, inter alia, cross selling, better product offering, research and marketing positioning.

This Policy, in conjunction with the FirstRand Group Privacy Minimum Standards, will serve as the basis for internal changes that are required to enable implementation of privacy requirements and compliance with privacy legislation requirements (such as the Data Protection Act, 2012, Act 843, Protection of Personal Information Act 4 of 2013 ("**POPIA**"), the EU General Data Protection Regulation, and the UK Data Protection Act of 2018), together with other applicable international legislation. The Policy will set the parameters to:

- position personal information ("**PI**") as a key asset;
- define a safe environment for safekeeping of PI;
- produce evidence that privacy compliance is applied;
- adhere to the regulatory environment requiring such compliance; and
- address the consequences that will follow in the event of a privacy incident occurring as a result of mismanagement of information in any manner.

First National Bank Ghana (FNBG) takes the higher of the home or host principle when dealing with South Africa where the parent company is based. This principle provides that when dealing with South Africa, laws and regulations which are of a higher standard than this Policy will take precedence over this Policy. However, where the Policy is of a higher standard it will take precedence. FNBG is required to comply with requirements in the Data Protection Act that is considered more onerous than stated in this Policy. In need, FNBG may apply for a deviation from the relevant Policy and the relevant deviation process will be followed.

The purpose of the FNBG Internal Privacy Policy ("**Policy**") is to outline the commitment of the bank as a good corporate citizen, to comply with the provisions of privacy legislation and regulation and to ensure that PI in the possession of FNBG, as well as PI collected by the bank is protected and secured against any unlawful collection, retention, dissemination and use. This Policy governs the handling of PI by FNBG and establishes a set of principles for the collection, retention, processing, dissemination and general good management of PI in the possession of the bank.

Furthermore, the Policy aims to protect the privacy rights of persons (both natural and juristic) in the instances where, the bank and/or any Operator that may process PI on FNBG's behalf, is processing personal information. Privacy legislation endeavours to balance, on the one hand, the fundamental right of the data subject to privacy and, on the other hand, the legitimate need of private and public bodies to obtain and process PI for various business-related purposes. This balance is achieved through universally accepted privacy principles or conditions which will be incorporated into the Policy. This Policy also includes general information regarding FNBG's treatment of past, present and prospective employees, customers and supplier's PI and their rights and responsibilities in respect of their PI.

In order to provide more context to the abovementioned statement and for the Policy reader to have a clear understanding of the following:

- what is regarded as personal information;
- who is regarded as the responsible party;
- who is considered to be a data subject;
- what is considered a record of such personal information; and
- what is considered processing of such personal information.

The definitions of these concepts are set out and fully explained in the definitions section of this Policy.

2. DEFINITIONS

The following concepts will be used throughout this Policy and are defined as follows:

Child	a child is a natural person who is defined as a child by a country's legislation and who has not been recognised as an adult by the courts of a country.
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 (like a parent or guardian).
Consent	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Customer	A customer is a natural or legal person who is an existing FNBG customer or a person who provided their personal or special personal information to the bank in the context of a sale of products or services, or is the successor in title of such customer or a beneficiary of such service (where the entities within FNBG are acting as joint responsible parties).
Data Protection Commission	means the independent national authority responsible for upholding the fundamental right of individuals to data privacy through the enforcement and monitoring of compliance with the Data Protection Act.
Data Subject	means the person to whom PI relates. In reference to FNBG this means, primarily but without limitation, customers; employees; operators/suppliers; other persons and third parties.
Employee	means a person employed for wages or salary, including permanent employees, non-permanent employees, past and prospective employees, contractors and contingent workers and for the purposes of this Policy including directors, non-executive directors and specialist consultants of FNBG.
First National Bank Ghana	means First National Bank Ghana Limited
Juristic Person	means an existing company, corporation, trust, not-for-profit organisation, or other legal entity recognised by law as having rights and duties.
Natural Person	means an identifiable, living human being.
Operator	means a person who processes PI for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that Responsible Party. This means any party that provides a service to process information on behalf of FNBG.
PAIA	Promotion of Access to Information Act 2 of 2000
Personal Information ("**PI**")	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 PI relating to the person or if the disclosure of the name itself would reveal information about the person. as defined in Protection of Personal Information Act 4 of 2013 or amendments thereto.
POPIA	Protection of Personal Information Act 4 of 2013
POPIA Regulations	Protection of Personal Information Act 4 of 2013 Regulations relating to the Protection of Personal Information
Privacy Minimum Standard	means minimum standards addressing the following matters, including but not limited to: 1. Privacy Incident Management; 2. Privacy control implementation; and 3. Confirming legitimate interest as a lawful justification for processing personal information.
FNBG Privacy Notices	means FNBG level privacy notices, including but not limited to: 1. The FNBG Customer Privacy Notice; 2. The FNBG Employee Privacy Notice; and 3. The FNBG Supplier and Business Partner Privacy Notices.
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.
Lawful Processing	means processing of personal information based on one of the lawful justifications as set out in the Data Protection Act.
Legitimate Interest	processing of personal information as set out in section (11)(1)(d) and/or section 11(1)(f) of POPIA.
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 anything 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; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Responsible Party/ies	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. In reference to this Policy, a Responsible Party would be a legal entity within FNBG that is registered and domiciled in Ghana or that is not domiciled in Ghana but makes use of automated or non-automated means in Ghana, to process personal information, and such processing extends beyond mere transmission of information through Ghana, and who

	determines the purpose and means for processing personal information, alone or in conjunction with others.
Special Personal Information ("**SPI**")	means any Personal Information of a data subject, concerning- (a) 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 (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Supplier	means a Natural or Juristic person that provides a product or renders services to FNBG.

3. APPLICABILITY AND SCOPE

3.1. All employees of FNBG have the responsibility of acquainting themselves with this Policy and the Privacy Minimum Standards, ensuring that they know, understand and comply with the provisions thereof. Failure to comply could result in significant risk to the bank and its business operations where PI, SPI and Children's PI are processed.

3.2. This Policy applies to all Fnbg entities; irrespective of jurisdiction; that process PI, SPI and Children's PI internally within Fnbg and to all Operators that process such information on behalf of the bank.

3.3. The PI, SPI and Children's PI being processed by FNBG may belong to, including but not limited to:

1. shareholders;
2. employees of FNBG
3. beneficiaries of employees, including children;
4. bursary students and interns;
5. customers of FNBG, including children irrespective of whether the product being offered to them is of a banking, banking related, insurance or other commercial nature;
6. beneficiaries of customers of FNBG, including children;
7. consultants;
8. contract workers;
9. non-executive directors;
10. business contacts; and
11. third party service providers/operators to FNBG and their employees.

3.4. This Policy applies to any device, system or business processes within FNBG information processing facilities and all PI, SPI or Children's PI, either new or existing, in electronic or paper-based form, or on any other media.

3.5. This Policy supports the:

1. FNBG Privacy Framework;
2. FirstRand Governance Framework in underpinning the King Code of Governance Principles for South Africa, 2016 ("King IV") principle relating to the effective management of information assets and ensuring that there are systems in place for the management of information and the management of information security;
3. Group Information and Technology Governance Framework providing the Group's approach regarding IT and IT security requirements;
4. FNBG Records Management Policy; and

5. FirstRand Information Governance Framework.

3.6. This Policy must be read in conjunction with applicable and relevant FNBG policies as communicated periodically.

3.7. Reference to PI in this document does not include reference to SPI and Children's PI.

4. PRINCIPLES APPLICABLE TO THE HANDLING OF PI AND SPI

4.1. FNBG will protect all PI, SPI and Children's PI in its possession and under its control in line with its contractual obligations, industry standards, professional requirements and internal policies, as well as applicable privacy and other law. In the event that a provision of this Policy conflicts with any other provisions or Policy then the provisions of this Policy will take precedence. In the event that the provisions of this Policy conflict with the law (including legislation and regulations), the law will take precedence over the Policy. The applicable privacy principles are as follows:

4.1.1. Privacy Principle 1: Accountability

4.1.1.1. FNBG will ensure that all processes and procedures that handle and deal with PI, SPI and Children's PI (from the collection, processing, dissemination, retention and destruction) comply with the Data Protection Act, 2012, Act 843 l and relevant international privacy legislation and regulation. In pursuance of compliance with these, the following will be established:

1. A privacy governance structure and formal privacy reporting (which will be addressed in the FNBG Privacy Framework);
2. A formal privacy Policy (this Policy) and supporting standards and practices;
3. A privacy framework (includes appropriate privacy roles, responsibilities and accountabilities).

4.1.1.2. The Responsible party within FNBG will depend on the nature of the processing and the data subject to whom the PI relates, but in relation to customer PI it will be the entity with whom the customer first contracts which entity would act in conjunction with other entities in FNBG as Responsible parties. All the customer facing entities must be listed in the bank's Customer Privacy Notice as Responsible parties.

4.1.1.3. FNBG will ensure that adequate contracts with operators are concluded which include appropriate protection obligations, where PI is processed by a third-party provider (operator).

4.1.1.4. The roles and responsibilities for Data Privacy Officers across the bank is defined in the FNBG Privacy Framework.

4.1.1.5. A formal bank wide privacy training awareness programme has been established and conducted at induction and on an on-going basis for employees.

4.1.2. Privacy Principle 2: Processing Limitation

4.1.2.1. FNBG will process PI of Data Subjects lawfully and, in a reasonable manner so that it does not unreasonably intrude on the Data Subject's right to privacy.

4.1.2.2. Collection of all PI and SPI will be directly from the Data Subject (or from the parent or legal guardian, in the case of a Child's PI or an authorised intermediary).

4.1.2.3. This means PI will be collected throughout the relationship with FNBG through various interactions including, but not limited to, collection required by law.

4.1.2.4. A Data Subject's PI may be collected from another party as long as the conditions in law are adhered to.

Minimality

4.1.2.5. FNBG will only process PI that is relevant, adequate and not excessive in relation to the purpose for which the information was collected.

Justification

4.1.2.6. To achieve transparency, a valid justification for the processing of PI will be disclosed by FNBG to Data Subjects, either before the collection of the PI or as soon as reasonably practical thereafter.

Consent and other lawful justifications to process PI, SPI and Children's PI

4.1.2.7. FNBG will ensure that PI is processed only where there is a lawful justification to do so. This may include where FNBG is required to process the PI to conclude and fulfil contractual terms or obligations, to comply with obligations imposed by law, to protect or pursue the Data Subject's or FNBG's legitimate interests, and where necessary in terms of Consent obtained from the Data Subject in line with the Data Protection Act, 2012, Act 843 and also in accordance with the following:

1. All Consent obtained is to be voluntary, specific and informed consent.
2. Prior to the processing of PI, SPI or Children's PI and if required as there is no other justification for the processing, FNBG must ensure that Consent has been obtained from the Data Subject or a Competent Person.
3. An appropriate record of the Consent obtained should be kept and be retrievable.
4. Consent for the processing of PI need not be obtained if:
   (a) necessary for the purpose of a contract to which the data subject is a party;
   (b) authorised or required by law;
   (c) to protect a legitimate interest of the data subject;
   (d) necessary for the proper performance of a statutory duty; or
   (e) necessary to pursue the legitimate interest of the data con- troller or a third party to whom the data is supplied.
   (f)
5. FNBG will process SPI with the Consent of the Data Subject or based on a lawful justification ground and will adhere to the limitations that apply to the processing of SPI (as outlined in this Policy and in the applicable Privacy Minimum Standard).
6. FNBG will process Children's PI with the Consent of a Competent Person in relation to a child or based on a lawful justification ground and will adhere to the limitations that apply to the processing of Children's PI (as outlined in privacy legislation, this Policy and in the applicable Privacy Minimum Standard).
7.

Lawful Justification Mechanisms for processing customer, employee and supplier PI and SPI by FNBG and its entities/subsidiaries

4.1.2.8. The privacy terms for Customers of FNBG should be incorporated in the contractual documentation presented to the Data Subject when being engaged for the first time.

4.1.2.9. FNBG must make the relevant Privacy Notice available to the Data Subject in an appropriate manner.

4.1.2.10. The privacy terms relating to Data Subjects who are employees of FNBG can be found in the FNBG Privacy Employee Declaration, which is incorporated into the FNBG HR Manual.

4.1.2.11. The privacy terms relating to Data Subjects who are third party service providers or suppliers of FNBG should be addressed in the agreement between FNBG and the Supplier.

Application of Legitimate Interest

4.1.2.12. Where the processing of PI is based upon the Legitimate Interest of the Responsible Party or the Data Subject; a legal justification must be provided, which supports the processing of the PI on this basis.

4.1.2.13. The legal justification referred to above, must be established by:

1. Conducting a Compatibility Assessment, to determine if the processing of the PI is compatible with the original purpose for collection and processing as mentioned in Principle 4 of this Policy, and a Legitimate Interest Assessment. The Legitimate Interest Assessment is a 3-component assessment consisting of a:
    - Purpose Assessment, to identify the Legitimate Interest of the Responsible Party or Data Subject;
    - Necessity Assessment, to determine if the processing is necessary for the purpose that has been identified; and
    - Balance Assessment, to determine if the processing has an impact on individuals' interests, rights and freedoms and to assess whether this overrides the Legitimate Interests of the Responsible Party.

4.1.2.14. The form and manner to carry out the above-mentioned assessments is set out in the applicable Privacy Minimum Standard.

4.1.2.15. The application of Legitimate Interest does not validate the further processing of PI for a purpose that is incompatible with the original purpose of collection and processing. Where the further processing is found to be incompatible with the original purpose of collection and processing, consent will be required unless other exceptions are applicable under such further processing, in line with Principle 4 of this Policy.

4.1.2.16. The application of Legitimate Interest does not guarantee compliance to the other privacy principles mentioned in this Policy, and as such the other privacy principles relating to minimality, purpose specification, restrictions of further processing etc. must also be complied with.

4.1.2.17. The application of Legitimate Interest does not exempt compliance with further requirements attached to the processing, such as Children's PI, direct marketing and automated decision making.

4.1.2.18. Where a Data Subject objects in terms of a stated Legitimate Interest, FNBG must establish whether such objection is reasonable, or unless legislation provides for such processing, before halting such processing.

Usage of the PI, SPI and Children's PI collected by FirstRand and its entities/subsidiaries

4.1.2.19. PI will be collected for a specific, explicitly defined and lawful purpose related to a function or business activity of FNBG. All Data Subjects, whose PI is processed, will be made aware of the purpose of the processing of their PI, as per Privacy Principle 6, Openness, of this Policy.

4.1.2.20. FNBG may only use the PI, SPI and Children's PI for the purposes as permitted by law and outlined in this Policy, the Privacy Minimum Standard, the relevant FNBG Privacy Notices, the FNBG Employee Privacy Notice and the FNBG Data Protection Policy for Suppliers and Business Partners.

4.1.2.21. FNBG may only use the PI for purposes as legally justified or where the Data Subject has provided Consent for the amended purpose or in cases where the Data Subject will not suffer prejudice by the change of purpose or as permitted by law.

Objection to the processing of PI and SPI by a Data Subject

4.1.2.22. In the event that a Data Subject (or Competent Person in relation to a Child) objects to the processing of their PI, SPI or Child's PI, FirstRand will stop processing that PI within a reasonable time unless there is an obligation for FNBG to continue processing the PI in order to comply with other legal, regulatory or contractual requirements. The Data Subject should be informed of the consequences of objection to processing, where these may exist.

4.1.2.23. Specific in-country requirements (as per law/regulations) relating to the manner in which a Data Subject can object to processing can be found in Annexure 1 of this Policy.

4.1.3. Privacy Principle 3: Purpose Specification

4.1.3.1. FNBG will only collect PI, SPI and Children's PI for a specified, explicitly defined, purpose which is lawful and related to a business activity of FNBG. This will be disclosed to the Data Subject when the PI, SPI or Children's PI is collected from the Data Subject or if collected from a third party, it will be disclosed as soon thereafter as reasonably possible.

Transparency and purpose for the processing of PI, SPI and Children's PI

4.1.3.2. FNBG will ensure that there is adequate transparency relating to the purpose for which a Data Subject's PI, SPI and/or Children's PI is to be collected and processed.

4.1.3.3. Such transparency and the purpose for the processing of PI, SPI and Children's PI, for Data Subjects who are customers of FNBG, will be specified in the FNBG Customer Privacy Notice, which must be accessible to such Data Subjects in a reasonable time and manner.

4.1.3.4. PI and SPI belonging to employees of FNNBG will be processed for the following purposes specified in the FNBG Employee Privacy Notice, including but not limited to: providing remuneration to the employees; opening a bank account on behalf of the employee; conducting criminal, credit, reference, and other related reference checks on the employee or prospective employee, carrying out the specific obligations and duties of FNBG in the field of employment legislation; realising objectives laid down by or by virtue of tax or other applicable legislation; properly assessing performance under an employment contract; undertaking management activities, such as succession planning, talent management, training, work planning, managing tasks, assessing the performance of the employees, and controlling security and access to facilities and rendering value added services to the employee, such as wellness (Medical aid, clinics etc.), catering services and other lawfully permitted purposes. In addition, the PI of the Children of employees may be processed when they are beneficiaries on Employee Insurance, Medical, Provident or Pension schemes. Such purposes must be evident in the FNBG Employee Privacy Notice.

Retention and destruction of PI, SPI and Children's PI

4.1.3.5. FNBG will not retain records of PI and SPI for excessive periods which are longer than necessary to achieve the stated purpose for processing, unless the retention of such PI, SPI and Children's PI is in accordance with the provisions of legislation or legitimate business purpose.

4.1.3.6. FNBG will ensure that all such records will be retained and safely destroyed in accordance with the FNBG Records Management Policy and Standards and Records Retention Schedule.

4.1.3.7. FNBG may retain records of PI, SPI or Children's PI beyond its stipulated retention period only for historical, statistical or research purposes, and such retention will be done in line with the applicable privacy and security safeguards of the bank

4.1.3.8. The FNBG Records Management Policy and Records Retention Schedule will be owned and maintained by Information Governance and can be accessed via the intranet in the Policy repository.

4.1.4. Privacy Principle 4: Further Processing

4.1.4.1. Further processing of a Data Subject's PI will only be permitted if this processing is compatible with the original purpose of collection and processing, as specified in the FNBG Customer Privacy Notice; the FNBG Employee Privacy Notice; and the FNBG Supplier and Business Partner Privacy Notice.

4.1.4.2. Where the original purpose for which the PI was collected and processed differs substantially from the purpose of the further processing, the Data Subject must be provided with an

opportunity to review the new purpose and consent to such further processing, unless another exception for further processing is available.

4.1.4.3. Further processing of PI, SPI and Children's PI will be allowed for the following reasons: if the Data Subject (or a competent person if the Data Subject is a Child) consents to the further processing, if obtained from a public record, or the PI was deliberately made public by the data subject, if further processing is required by law, to protect a public interest or matters of national security, or by authorisation of the applicable Data Protection Authority.

4.1.5. Privacy Principle 5: Information Quality

4.1.5.1. FNBG must take all reasonable steps to ensure that PI, SPI and Children's PI processed or under their control is complete, accurate, not misleading and updated when necessary.

4.1.5.2. FNBG must ensure that channels are available for customers to update their PI in the event that it changes.

4.1.5.3. FNBG will take all reasonable steps to provide means for employees to update their PI by providing and maintaining a self-service channel, through which employees are required to update PI when it changes. For updates to employee PI that cannot be made through a self-service channel, employees are required to address the relevant request to the responsible HR Department.

4.1.6. Privacy Principle 6: Openness

4.1.6.1. FNBG will allow access to information in terms of the provisions of the Data Protection Act, 2012, Act 843

4.1.6.2. FNBG must take all reasonable steps to ensure that Data Subjects are aware of the PI, SPI and Children's PI that is collected, the purpose of the collection, how long the information will be retained and the parties with whom the information is shared. Such information must be clearly articulated in the FNBG Customer Privacy Notice, the FNBG Employee Privacy Notice and the FNBG Supplier and Business Partner Privacy Notice.

4.1.6.3. FNBG1 will make available to the Data Subject: the name and address of the Responsible Party, the business within FNBG requiring the information; the purposes for which the information is collected; whether or not the supply of the information required is mandatory or voluntary; the consequences of the failure of the Data Subject to provide such information; the legal requirement for collection of the information, and any further information ensuring reasonable processing of the Data Subject's information such as the recipient or categories of recipients of the information; nature or category of the information; any right to access the information; and the existence of any right of access to update/amend the information..

4.1.7. Privacy Principle 7: Security Safeguards

4.1.7.1. FNBG will ensure the integrity and confidentiality of PI, SPI and Children's PI in its possession, or under its control, by taking appropriate, reasonable, technical and organisational measures to prevent loss, damage and unauthorised access to or destruction of PI. Such measures must include the prevention and timely detection of unauthorised access to PI, SPI and Children's PI; and the protection of computer systems and networks used for storing, processing and transmitting PI, SPI and Children's PI.

4.1.7.2. All PI, SPI and Children's PI, will be handled by FNBG, in terms of the FirstRand Group Information Security Policies and Group Information Security Minimum Standards.

4.1.7.3. FNBG must ensure that all permanent and non-permanent employees, including contractors are trained on measures to prevent loss, damage and unauthorised access or destruction of PI, SPI and Children's PI under its control.

4.1.7.4. Taking into account that PI, SPI and Children's PI is processed on behalf of FNBG by third party service providers/Operators, these service providers/Operators are also bound and

committed to the privacy requirements which must be instituted in the form of non-disclosure agreements, confidentiality and data protection clauses in service agreements.

4.1.7.5. FNBG will, as part of its information risk management process, take cognisance of the industry requirements relating to generally acceptable information security practices and procedures in terms of specific local and/or global industry or professional rules and regulations.

4.1.7.6. FNBG will ensure that internal and external information security risks to PI, SPI and Children's PI in its possession are identified on a continuous basis. Moreover, FNBGwill ensure that the appropriate safeguards are established and maintained against the identified risks and regular verification of the effective implementation of such safeguards will be undertaken and continuously reviewed and updated in response to new risks.

4.1.7.7. FNBG will put in place internal processes and procedures with clearly defined roles and responsibilities to discover or identify the presence or existence of, record and manage security compromises as they arise in line with the Privacy Minimum Standard relating to privacy incident management; the operating standards and procedures relating to privacy incident management and cyber incident management processes. Where relevant, such incidents must be reported to the relevant Data Protection Authority and the affected data subjects in terms of the Data Protection Act.

4.1.7.8. FNBG will ensure that its automated decision-making processes do provide for a manual referral in need and will ensure that for any directory of subscribers a data subject will be informed, free of charge and before any information is in included in the directory.

4.1.8. Privacy Principle 8: Data Subject Participation

4.1.8.1. FNBG will ensure that it has processes in place whereby data subjects can enquire as to what information FNBG holds on them.

4.1.8.2. Data Subjects have the right to be provided with their PI, SPI and Children's PI and have the information corrected if it is inaccurate, irrelevant, excessive, incomplete, misleading or has been obtained unlawfully.

4.1.8.3. Further to that, FNBG accepts that data subjects have the right to object to receiving marketing material from FNBG. This will be done according to the FNBG Direct Marketing Consent Policy.

4.1.8.4. FNBG must implement the required channels that enable data subjects (customers, employees or suppliers) to approach FNBG as stipulated in the Data Protection Act, in order for FNBG to confirm whether it holds PI or SPI about the data subject, free of charge. Moreover, FNBG will be required to provide the record or a description of the PI or SPI held by FNBGd, or an Operator, within a reasonable period of time; in the prescribed format, and may levy the prescribed charges.. Where FNBG provided a record or description of the PI or SPI, the bank will advise the Data Subject that they may request a correction or deletion of the information. Such correction or deletion of the PI or SPI will be entertained by FNBG if the PI or SPI is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, and in line with the applicable legislative requirements.

4.1.8.5. Subject to Privacy regulations, FNBG has in place a Complaints Handling Policy which outlines the manner for receiving and investigating privacy related complaints; and co-operating with the Data Protection Commission on such complaints.

4.1.8.6. Requirements (as per law/regulations) relating to the manner in which a data subject can request for their PI or SPI to be corrected or deleted can be found in Annexure 1 of this Policy.

4.1.9. Privacy Principle 9: Cross Border Transfer of Personal Information

PI, SPI and Children's PI in the possession of FNBG may be transferred to a third party in another country if:

- The PI will be adequately protected under the other country's laws or an agreement with the third-party recipient;

- Where the transfer is necessary to enter into or perform under a contract with a data subject, or a contract with a third party that is in the data subject's interest;
- Where the data subject has consented to the transfer; or
- Where it is not reasonably practical to obtain the data subject's consent, but the transfer is in the data subject's interest.

4.1.9.1. All cross-border transfers of PI will be subject to the terms of this Privacy Policy, the Privacy Minimum Standard and the Data Protection Act and other applicable legislation and legal requirements.

4.1.9.2. Prior authorisation of the Data Protection Commission must be obtained for this processing where the law requires.

4.1.10. Privacy Principle 10: Third Party / Operator Management

4.1.10.1. FNBG will ensure that third party suppliers/operators processing any PI on its behalf have adequate technical and organisational measures to prevent loss, damage and unauthorised access to or destruction of FNBG PI under the control of the third-party service provider or operator by means of conclusion of a contract.

4.1.10.2. Such measures for third party service suppliers or operators must be in line with this Policy, the applicable Privacy Minimum Standard and FirstRand Information Security Policies and Standards

4.1.10.3. Regular monitoring of third-party suppliers or operators will be undertaken by FNBG, to ensure that the PI handled by the third-party supplier or operator is dealt with legally and in accordance with the aforementioned policies and standards as when required.

4.1.10.4. The FNBG Data Protection Policy for Suppliers and Business Partners must include contractual provisions relating to confidentiality of personal information; processing limitations; legal requirements, incident reporting and termination provisions for third party suppliers or operators.

5. GENERAL

5.1. Non-compliance with this Policy and all related policies, standards, procedures and directives may result in disciplinary action or dismissal.

5.2. In addition, the penalties for non-compliance ranges from:

- Administrative fines of up to 5000 penalty units (GHS60,000)
- Imprisonment of up to 10 years
- Penalties from more than one jurisdiction may also apply.

6. OWNERSHIP AND REVIEW

6.1. This Policy is owned by Compliance and must be reviewed at least every two (2) years. This Policy will also be reviewed as a result of any privacy legislative change (including regulatory guidelines and industry codes of conduct).

ANNEXURE 1: SPECIFIC IN-COUNTRY REQUIREMENTS RELATING TO DATA SUBJECT RIGHTS

1.1. Objection to the processing of PI and SPI by a Data Subject

1.1.1. Unless otherwise provided by law, a data subject may object to the processing of personal data.

1.1.2. Where a data subject objects to the processing of personal data, the person who processes the personal data shall stop the processing of the personal data.

1.2. Correction or deletion of PI or destruction or deletion of record of Personal Information

(1) A data subject may request a data controller to
(a) correct or delete personal data about the data subject held by or under the control of the data controller that is inac- curate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or
(b) destroy or delete a record of personal data about the data subject held by the data controller that the data controller no longer has the authorisation to retain.

(2) On receipt of the request, the data controller shall comply with the request or provide the data subject with credible evidence in support of the data.
(3) Where the data controller and the data subject are unable to reach an agreement and if the data subject makes a request, the data con- troller shall attach to the record an indication that a request for the data has been made but has not been complied with.
(4) Where the data controller complies with the request, the data controller shall inform each person to whom the personal data has been disclosed of the correction made.
(5) The data controller shall notify the data subject of the action taken as a result of the request.

-END-