FirstRand

PRIVACY NOTICE

The Privacy notice contains the employee, customer, and supplier privacy notices, as well as locations for the in-country and local privacy notices.

FirstRand and its brands

Privacy notice type	Location (Refer to the annexures below or copy and paste the URL in your internet browser)
Employee	Refer to Annexure A below
Customer	https://www.firstrand.co.za/media/investors/policies-and-practice/pdf/group-customer-privacy-notice-2023.pdf
Supplier	https://www.firstrand.co.za/media/investors/governance/firstrand-group-supplier-privacy-notice.pdf
Website	www.firstrand.co.za

Broader Africa

Privacy notice type	Location (Refer to the annexures below or copy and paste the URL in your internet browser)
Botswana	
Customer	https://www.fnbbotswana.co.bw/downloads/fnbBotswana/legal-matters/privacyPolicy/CustomerPrivacyNotice.pdf
Employee	Refer to Annexure B below
Website	www.fnbbotswana.co.bw
Ghana	
Customer	https://www.firstnationalbank.com.gh/legal/privacyPolicy.html
Employee	Refer to Annexure C below or follow the link: https://www.firstnationalbank.com.gh/downloads/Ghana/InternalPrivacyPolicyCookieNotice.pdf
Website	www.firstnationalbank.com.gh
Namibia	
Customer	https://www.fnbnamibia.com.na/downloads/namibia/2022/FirstRandNamibiaGroupCustomerPrivacyNotice.pdf
Employee	Refer to Annexure D below
Website	www.fnbnamibia.co.na

Privacy notice type	Location (Refer to the annexures below or copy and paste the URL in your internet browser)
Lesotho	
Customer	https://www.fnb.co.ls/downloads/Lesotho/legal-matters/privacyPolicy/FNBLesothoCookiePrivacyNotice.pdf
Employee	Refer to Annexure E below
Website	www.fnb.co.ls
Mozambique	
Employee	Refer to Annexure F below
Website	www.fnb.co.mz
Mauritius	
Employee	Refer to Annexure G below
Zambia	
Customer	https://www.fnbzambia.co.zm/downloads/zambia/ViewCustomerPrivacyNotice.pdf
Employee	Refer to Annexure H below
Website	www.fnbzambia.co.zm
Eswatini	
Customer	https://www.fnbswaziland.co.sz/downloads/swaziland/CustomerPrivacyNotice.pdf
Employee	Refer to Annexure I below
Website	www.fnb.swaziland.co.sz
Nigeria	
Customer	https://www.rmb.com.ng/files/pdf/other/rmb-nigeria-private-policy.pdf
Employee	Refer to Annexure J below
Website	www.rmb.com.ng

United Kingdom (UK) and United States (US) – (RMB, FNB and Aldermore)

Privacy notice type	Location (Refer to the annexures below or copy and paste the URL in your internet browser)
England - UK	
Customer	https://www.aldermore.co.uk/legal/privacy-policy/
Employee	Refer to Annexure K below
Website	www.aldermore.co.uk
US	
Customer	https://www.rmbsecurities.com/page/privacy-notice
Website	www.rmbsecurities.com

Privacy notice type	Location (Refer to the annexures below or copy and paste the URL in your internet browser)
Jersey	
Employee	Refer to Annexure L below

Other – Volkswagen (VW)

Privacy notice type	Location (Refer to the annexures below or copy and paste the URL in your internet browser)
Customer	https://www.vw.co.za/en/volkswagen-experience/corporate-information/privacy.html
Employee	Refer to Annexure M below
Website	www.vw.co.za

Any related queries may be emailed to ethicsoffice@firstrand.co.za.

Group Ethics and Governance Office

FirstRand

FIRSTRAND GROUP EMPLOYEE PRIVACY NOTICE

October 2021

DOCUMENT CONTROL

Title	FirstRand group employee privacy notice
Authors	Group Compliance
Document version	0.6
Version date	1 October 2021
Approval	Approved by the FirstRand data and privacy committee.
Date of next review	October 2023

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE

Protecting the privacy of the personal information of its employees is very important to FirstRand and it follows general principles in accordance with applicable privacy laws and, particularly, the Protection of Personal Information Act (POPIA).

This group employee privacy notice (the **notice**) has been developed to help group employees understand how FirstRand collects, uses and safeguards their personal information.

FirstRand's notice includes general information regarding FirstRand's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information. FirstRand's notice incorporates, by reference, FirstRand's acceptable use of information resources policy.

2 SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past and prospective employees (that is, permanent and temporary employees), as well as fixed-term contractors or independent contractors contracted by the FirstRand group. This notice also applies to persons who interact with the group's human resources platform.

3 DISCLOSURE INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION

FirstRand will process personal information collected from group employees. Certain personal information-processing activities may be outsourced to third parties, and FirstRand and the third party will adhere to the conditions included in paragraphs 3.8 and 3.9 below.

3.1 Responsible parties in FirstRand

In this notice, **FirstRand** or **the group** means FirstRand Limited and its South African subsidiaries (as defined in the Companies Act 71 of 2008, including divisions, segments and business units), but specifically excludes subsidiaries, where such entity is a subsidiary as a result of an investment by any one of RMB's private equity businesses (predominantly legally structured under FirstRand Investment Holdings (Pty) Ltd). However, this notice may apply to the above-mentioned excluded subsidiaries and other companies associated with FirstRand if agreed to by FirstRand and the relevant subsidiary or associated entity in writing. Confirmation as to whether this notice applies to a specific entity associated with FirstRand can be sought through the mechanisms set out in this notice.

Depending on the processing practice in question, the companies in the FirstRand group, as listed on the FirstRand website under ownership and legal structure at https://www.firstrand.co.za/the-group/ownership-and-legal-structure/, may act as responsible parties. In this notice, any reference to "the group" or "FirstRand" includes any one or more (if they are acting jointly) of the FirstRand companies, and all affiliates, associates, cessionaries, delegates, successors in title, or third parties (authorised agents and contractors) when such parties are acting as responsible parties, joint responsible parties or operators in terms of applicable privacy laws, unless stated otherwise.

3.2 Definition of employees' personal information

For the purpose of this notice and other documents referred to in this notice, personal information means information about an identifiable, living, natural person.

By way of example, an employee's personal information and special personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status,

disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private and/or confidential.

Personal information does not include aggregated or anonymised information where FirstRand is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee which may be included as part of a statement about a group of employees, or a graph or pie chart showing characteristics of a group of employees only. For instance, *"Twenty per cent of FirstRand's employees own or use a laptop computer"* is not personal information.

Personal information processed by FirstRand regarding group employees includes the following types of information:

- personal details, including but not limited to name, address, location information, online identifier, emergency contact details, birth certificate number, employee number, identity number, age, marital status, language, financial history, criminal history, employment history, educational history and other qualifications;
- job-related details, e.g. starting date, place of work, salary, benefits and absence records;
- financial information, e.g. bank account numbers; and
- performance/evaluation information, e.g. whether an employee performs job duties in accordance with the relevant requirements.

An employee undertakes to communicate their personal information to FirstRand when specifically requested by FirstRand to do so.

3.3 Definition of employees' special personal information

There are special categories of an employee's personal information which FirstRand will only process where a more stringent set of requirements are met. These special categories are information revealing:

- religion or philosophical beliefs, for relevant holidays or catering for specific dietary requirements;
- pregnancy, for relevant leave;
- disability, for employment equity and catering for specific needs;
- biometric information, for identification, verification and access to premises and platforms;
- health information, for Covid-19 (pandemic) measures, adherence to various health protocols, leave and claims, amongst others;
- race or ethnic origin;
- trade union membership;
- political persuasion; and
- certain information relating to criminal offences and criminal behaviour.

It is important to note that the processing purposes identified above are not exhaustive and other lawful processing may also take place.

The group processes medical and health-related information with the employee's consent, for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for their benefit, and in order to comply with FirstRand's obligations under the Occupational Health and Safety Act 181 of 1993. In certain circumstances an employee's special personal information may also be required and consent obtained in order for the group to assess, submit and manage insurance claims for, on behalf of, or in relation to such employees or the employees' beneficiaries.

The group will not retain or process special personal information unless one of the statutory exceptions applies. For example (where a statutory exception is to obtain consent), specific consent relevant to the processing of biometric personal information may be requested by the group.

3.4 Purposes of the processing of personal information

Personal information will be processed by the group in the normal course of business of managing employees for various purposes, including but not limited to the following:

- for required banking information in order to process an employee's remuneration;
- to suggest the opening of a bank account on behalf of the employee, in order to secure staff rates;
- to admit the employee (and beneficiaries) to the FirstRand retirement benefit structure and/or FirstRand Retirement Fund or RMB Provident Fund, and ensure administration thereof (may include the personal information of the employee's beneficiaries);
- to admit the employee and dependants to medical aid providers, provide a subsidy where applicable and provide the relevant administration (may include the personal information of the employee's dependants);
- to keep proof of medical aid membership in cases where employees elect to be a dependant on another person's scheme other than FirstRand medical aid providers in order to comply with a condition of employment;
- to comply with the group's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented by the group. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the employee, including but not limited to the Register of Employees Dishonesty System (REDS), politically exposed person, Southern African Fraud Prevention Service, Association for Savings and Investment South Africa and Financial Advisory and Intermediary Services Act reference checks. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits, as well as reporting on the conduct of employees where required to do so by law, to the relevant bodies after termination of employment;
- to comply with all applicable laws authorising or requiring such processing, including (but not limited to) the Basic Conditions of Employment Act 75 of 1997; the Labour Relations Act 66 of 1995; the Employment Equity Act 55 of 1998; the Occupational Health and Safety Act 85 of 1993; the Financial Intelligence Centre Act, 2001; the Prevention and Combating of Corrupt Activities Act 12 of 2004 and the Companies Act 71 of 2008, and their regulations;
- to carry out the specific obligations and duties of FirstRand in the field of employment legislation;
- to realise objectives laid down by or existing by virtue of tax or other applicable legislation;
- to properly assess performance under an employment contract;
- to undertake management activities, such as succession planning, talent management, training, work planning, managing tasks, assessing the performance of employees, and controlling security and access to facilities;
- to market products, goods and services to the employee, and to track the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels and research for statistical purposes and/or the creation of employee-specific product offerings; and/or
- otherwise securing and facilitating the employee's employment with the group, including rendering to the employee value-added services (such as employee wellness initiatives and catering services), employee administration, training, performance reviews, talent management and other tasks=s related to the management of employees;
- to share employee/partner/child(ren) personal information for business purposes, e.g. for business travel, events, delivery or collection of gifts, group assets or packages;

- to share children's details, e.g. beneficiaries of pensions on the death of a parent, or if the parent signs the child(ren) up for volunteer project benefits or other promotions or benefits offered by the group from time to time;
- to share close relatives' details – for example emergency contact persons;
- to compile statistics and results from research studies and related programmes;
- to send work-related communications to the employee's mobile device; and/or
- for any other related purposes.

The purposes above indicate the cases where it is mandatory for employees to provide their personal information to enable the processing of:

- the performance of the employment contract to which the employee is party, or in order to take steps at the request of the prospective employee prior to entering into the employment contract; or
- compliance with the legal obligations to which the group is subject; or
- the protection of a legitimate interest of the employee; or
- the legitimate interests pursued by the group, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

- for a prospective employee: to the group being unable to enter into an employment contract with that prospective employee, and
- for an employee: to disciplinary sanctions, where applicable, or in extreme cases such refusal may lead to dismissal.

There may be instances where the group will lawfully process personal information for purposes not listed above. Where the provision of personal information does not fall within one of the lawful justifications for processing, separate consent from the employee (which consent may at any moment be withdrawn) will be sought.

3.5 Quality of personal information

FirstRand will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate, not misleading, and updated where necessary.

The group human capital functions have provided the self-service channels by means of which employees are required to update personal information if it changes. The onus is on the employee to utilise these channels to update their personal information, when necessary.

For updates of personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

3.6 Security and confidentiality of personal information

All personal information processed by FirstRand will be held confidential.

FirstRand will implement reasonable and appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

3.7 Retention of personal information

Personal information will not be kept by the group for longer than is necessary for the purposes of the processing as set out above, unless a further retention period is required by law, or where FirstRand reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and the group.

Other than in the aforementioned instances, the group may request the employee's consent for the further retention of personal information and will state the reasons for such a request.

3.8 The transfer of personal information

Employees' personal information may be shared within the group and with third parties with whom FirstRand contracts to process such personal information and pursuant to the instruction of FirstRand, under specific terms or terms as set forth in this notice for the purposes mentioned above. A simplified legal entity group structure is available on FirstRand's website under ownership and legal structure at https://www.firstrand.co.za/the-group/ownership-and-legal-structure/.

Provided that FirstRand ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of FirstRand and in accordance with this notice, FirstRand may transfer personal information within the group, to operators (see 3.9 below) or to other third parties based outside South Africa with whom the group has a lawful justification, e.g. parties who signed contracts requiring the other party to adhere to such standards of security and responsible handling in respect of the personal information as adhered to by the group, regardless of whether the laws of the countries in which such third parties reside provide sufficient safeguards regarding the processing of personal information.

3.9 Use of operators

An operator is a person who processes personal information on behalf of the group in terms of a contract or mandate, without coming under the direct authority of the group.

The group may assign the processing of group employee personal information to an operator, who will process the personal information only with the knowledge or authorisation of FirstRand.

The group will contract with the operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by the group.

3.10 Employees' privacy rights

3.10.1 Access to information

The employee has the right to access the personal information which relates to them. Where an employee wishes to request personal information which they do not have a direct right to, but which information is needed to protect a right of the employee, a request must be addressed in accordance with the procedure referred to in FirstRand's manual prepared in accordance with section 51 of the Promotion of Access to Information Act 2 of 2000.

This manual may be obtained on the FirstRand website at https://www.firstrand.co.za/investors/governance-and-compliance/. Certain personal information relevant to the employee may be accessed through the self-service channels.

3.10.2 Right to correction of personal information

The employee has the right to correct inaccurate personal information which relates to them. The employee is able to update and correct certain types of personal information stored on the human capital platform using the self-service

channel. For instructions on how to do so, the employee should contact the responsible person in their human capital department.

For updating other types of personal information, the employee should address a request to that effect to the responsible human capital department. Should the group be unable to correct the personal information, it must explain its position in writing to the employee.

Should the group refuse the correction, the employee is entitled to request that a statement be attached to the personal information which indicates that a correction had been sought and was not made.

3.10.3 Right to de-identification/destruction/deletion

The employee is entitled to require the de-identification/destruction/deletion of his/her/their personal information which is, by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete or misleading, or which had been obtained unlawfully;
- legally prohibited from being recorded, communicated or retained, or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a request to that effect to the responsible human capital department.

The group must delete/remove/destroy this personal information or explain in writing its position regarding the request. Should the group refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the personal information which indicates that a request for de-identification/destruction/deletion of personal information had been sought and was not made. The employer's statement should set out the summary for such refusal.

3.10.4 Right to complain

Employees have the right to submit a complaint to the Information Regulator regarding an alleged breach of the conditions for lawful processing of personal information as set out in POPIA. The Information Regulator's details can be found on the Information Regulator website at https://www.justice.gov.za/inforeg/contact.html.

An employee can choose to submit a complaint to the group for resolution before submission to the Information Regulator. Any queries or complaints regarding the employee's personal information can be directed to the relevant human capital manager within the group.

3.11 Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice, and for access to information about his, her or their personal information processed within the context of this notice, the employee may contact their data privacy officer, line manager or their human capital department.

The group must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

3.12 Other relevant group policies

- The FirstRand acceptable use of information resources policy, which is available at https://firstrandgroup.sharepoint.com/sites/FCCERM/ITGovernance/SitePages/Policies.aspx. This policy aims to ensure effective, efficient and secure use of the group's information resources, and informs employees of what is

deemed acceptable and unacceptable practice. Subject to the terms of this notice, the group will monitor the use of its information resources by employees.

- The FirstRand internal privacy policy.
- The FirstRand privacy framework.

1 BOTSWANA EMPLOYEE CODE OF CONDUCT – Extract of 2.5 and 2.6

2.5 Secrecy

Bank customers have the right to expect that all their dealings with the Bank, and any information relating to them which the Bank obtains, will be treated in the strictest confidence.

All information obtained by an employee during the course of his employment with the Bank is confidential. Strict secrecy shall be observed by all employees when dealing with such information, and employee may neither communicate nor allow to be communicated, any information made available to them in their capacity as employees of the Bank unless instructed to do so by a Manager of competent authority ('the Manager') or by a Court of Law or lawfully established Regulatory Authority.

Where an employee is, or has been required by a Court of Law or lawfully established Regulatory Authority to furnish or disclose confidential information, the concerned employee shall immediately notify the Manager and the Head of Legal in writing of such requirement.

No employee, unless authorised to do so by the Manager or by a Court of Law, shall allow any person who is not employed by the Bank to gain access to any books, documents or computer files/reports of the Bank, other than in the normal course of business. Where right of access is in doubt, the Manager shall refer the matter to the Head of Legal.

No employees shall, without the approval of the Manager, remove any books, records, papers, computer records/files or other written documents relating to the activities of the Bank or its clients, from the premises of the Bank.

Other than as part of the Conditions of Employment, employees shall be required to sign a Declaration of Secrecy on their first appointment, and at such other times as the Bank may require.

Any breach of secrecy shall be treated as a serious offence, and the employee concerned may be liable for summary dismissal.

2.6 Data Privacy

Confidential information must not be disclosed except to those internal or external parties who have a valid reason for receiving such information, such as to meet risk management, legal, and compliance needs, etc.

Confidential Information obtained from employees, prospective employees, or other third party is to be used only for the specific purpose for which it was given, except as provided above or otherwise agreed with employee/prospective employee.

All client employee information is confidential and may only be shared on a need-to-know basis. When determining whether to release confidential information, employees should always keep specific laws, as well as any agreed restrictions that may limit the release as prescribed in the Data Privacy law.

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

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-

FirstRand
NAMIBIA

FIRSTRAND NAMIBIA EMPLOYEE PRIVACY NOTICE

April 2024

DOCUMENT CONTROL

Document Information		
Document Title	FirstRand Namibia Employee Privacy Notice	
Document Level	Notice	
Version	2	
Effective Date	Upon approval at Policy Committee	
Document Permission	Internal	
Document Approval		
Document Owner	*Shaun van Rooi* *Chief Compliance Officer – FirstRand Namibia* *@Parkside, 130 Independence Avenue, Windhoek, Namibia* *Shaun.VanRooi@fnbnamibia.com.na*	
Review & Approval Process	**Compliance and Conduct Risk Committee** Review and Recommend for Approval	12 April 2024
	Policy Committee Approve	23 April 2024
	Enterprise Risk Management Committee Note	
Document Status	Reviewed	
Approval / Last Review Date	July 2020	
Date of Next Review	Every 3 years (or as and when material changes are required).	

Document Change Control			
Version	**Date**	**Author**	**Summary of Changes**
2.0	*12/4/24*	*Lize-Mari McNish*	- Aligned to in-country template. - Replaced FirstRand with Firstrand Namibia / FSRN. - Scope: - Included "This notice also applies to persons who interact with the group's human resources platform". - Disclosure: - Included "Certain personal information-processing activities may be outsourced to third parties, and FSRN and the third party will adhere to the conditions included in paragraphs 3.8 and 3.9 below". - Included "In this notice, references to "FSRN" or "the group" are to FirstRand Namibia Limited and its subsidiary companies, including its divisions, segments, and business units. Certain subsidiary companies may be excluded from the group description for the purposes of this privacy notice (such as where the group is involved in private equity investments). Confirmation as to whether this privacy notice applies to a specific company (a registered legal entity) associated with the group can be sought through the mechanisms set out in this notice"

			under 3.1. - Included “age, marital status, language, financial history, criminal history, employment history” under 3.2. - Included “In certain circumstances an employee’s special personal information may also be required and consent obtained for the group to assess, submit, and manage insurance claims for, on behalf of, or in relation to such employees or the employees’ beneficiaries” under 3.3. - Included “To admit the employee and dependents to medical aid providers, provide a subsidy where applicable and provide the relevant administration (may include the personal information of the employee’s dependents). To keep proof of medical aid membership in cases where employees elect to be a dependent on another person’s scheme other than FSRN medical aid providers to comply with a condition of employment” under 3.4. - Included “delivery or collection of gifts, Group assets or packages” under 3.4. - Included “or if the parent signs the child(ren) up for volunteer project benefits or other promotions or benefits offered by the group from time to time” under 3.4.

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE

Protecting the privacy of the personal information of its employees is very important to FirstRand Namibia (hereafter FSRN or the group) and it follows general principles in accordance with applicable privacy laws and, particularly, FSRN's policies in this regard.

This FSRN Employee Privacy Notice (hereafter the notice) has been developed to help Group employees understand how FSRN collects, uses, and safeguards their personal information.

The notice includes general information regarding FSRN's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information. FSRN's notice incorporates, by reference, FSRN's Ethical Use of Data Framework.

2. SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past, and prospective employees (that is, permanent and temporary employees), as well as fixed-term contractors or independent contractors contracted by the group. This notice also applies to persons who interact with the group's human resources platform.

3. DISCLOSURE INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION

FSRN will process personal information collected from Group employees. Certain personal information-processing activities may be outsourced to third parties, and FSRN and the third party will adhere to the conditions included in paragraphs 3.8 and 3.9 below.

3.1. Responsible parties in FirstRand Namibia

In this notice, references to "FSRN" or "the group" are to FirstRand Namibia Limited and its subsidiary companies, including its divisions, segments, and business units. Certain subsidiary companies may be excluded from the group description for the purposes of this privacy notice (such as where the group is involved in private equity investments). Confirmation as to whether this privacy notice applies to a specific company (a registered legal entity) associated with the group can be sought through the mechanisms set out in this notice.

In this privacy notice, any reference to ""FSRN" or "the group" includes any one or more (if they are acting jointly) Group companies and all affiliates, associates, cessionaries, delegates, successors in title or third parties (authorised agents and contractors), when such parties are acting as responsible parties, joint responsible parties, or operators in terms of applicable privacy laws, unless stated otherwise.

Depending on the processing practice in question, the companies in the group, as listed on the FirstRand Namibia website under ownership and legal structure at https://www.firstrandnamibia.com.na/about/ownership-and-legal-structure/, may act as responsible parties.

3.2. Definition of employees' personal information

For this notice and other documents referred to in this notice, personal information means information about an

identifiable, living, natural person.

By way of example, an employee's personal information and special personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private and/or confidential.

Personal information does not include aggregated or anonymised information where FSRN is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee which may be included as part of a statement about a group of employees, or a graph or pie chart showing characteristics of a group of employees only. For instance, *"Twenty per cent of* FSRN*'s employees own or use a laptop computer"* is not personal information.

Personal information processed by FSRN regarding Group employees includes the following types of information:

- Personal details, including but not limited to name, address, location information, online identifier, emergency contact details, birth certificate number, employee number, identity number, age, marital status, language, financial history, criminal history, employment history, educational history, and other qualifications.
- Job-related details, e.g., starting date, place of work, salary, benefits, and absence records.
- Financial information, e.g. bank account numbers.
- Performance/evaluation information, e.g. whether an employee performs job duties in accordance with the relevant requirements.

An employee undertakes to communicate their personal information to FSRN when specifically requested by FSRN to do so.

3.3. Definition of employees' special personal information

There are special categories of an employee's personal information which FSRN will only process where a more stringent set of requirements are met. These special categories are information revealing:

- Religion or philosophical beliefs, for relevant holidays or catering for specific dietary requirements.
- Pregnancy, for relevant leave.
- Disability, for employment equity and catering for specific needs.
- Biometric information, for identification, verification and access to premises and platforms.
- Health information, for Covid-19 (pandemic) measures, adherence to various health protocols, leave and claims, amongst others.
- Race or ethnic origin.
- Trade union membership.
- Political persuasion.
- Certain information relating to criminal offences and criminal behaviour.

It is important to note that the processing purposes identified above are not exhaustive and other lawful processing may also take place.

The group processes medical and health-related information with the employee's consent, for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for their benefit, and to comply with FSRN's obligations under the law. In certain circumstances an employee's special personal information may also be required and consent obtained for the group to assess, submit, and manage insurance claims for, on behalf of, or in relation to such employees or the employees' beneficiaries.

The group will not retain or process special personal information unless one of the statutory exceptions applies. For example (where a statutory exception is to obtain consent), specific consent relevant to the processing of biometric personal information may be requested by the group.

3.4. Purposes of the processing of personal information

Personal information will be processed by the group in the normal course of business of managing employees for various purposes, including but not limited to the following:

- For required banking information to process an employee's remuneration.
- To suggest the opening of a bank account on behalf of the employee, to secure staff rates.
- To admit the employee (and beneficiaries) to the relevant retirement benefit structure and/or retirement fund or provident fund and ensure administration thereof (may include the personal information of the employee's beneficiaries).
- To admit the employee and dependents to medical aid providers, provide a subsidy where applicable and provide the relevant administration (may include the personal information of the employee's dependents).
- To keep proof of medical aid membership in cases where employees elect to be a dependent on another person's scheme other than FSRN medical aid providers to comply with a condition of employment.
- To comply with the group's anti-money laundering, terrorist financing, fraud, and corruption detection obligations as well as risk management processes implemented by the group. This will include conducting criminal, credit, reference, sanctions, anti-bribery, and other related reference checks on the employee, including but not limited to the Register of Employees Dishonesty System (REDS), politically exposed person (PEP), relevant fraud prevention agencies and services and reference checks. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits, as well as reporting on the conduct of employees where required to do so by law, to the relevant bodies after termination of employment.
- To comply with all applicable laws authorising or requiring such processing, including (but not limited to): all employment and labour related laws, laws relating to the safety of employees as work and laws relating to financial crime, fraud, money laundering, KYC, sanctions, combatting of crime and corruption and other corporate laws and their regulations.
- To carry out the specific obligations and duties of FSRN in the field of employment legislation.
- To realise objectives laid down by or existing by virtue of tax or other applicable legislation.
- To properly assess performance under an employment contract.
- To undertake management activities, such as succession planning, talent management, training, work planning, managing tasks, assessing the performance of employees, and controlling security and access

to facilities.

- To market products, goods and services to the employee, and to track the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels and research for statistical purposes and/or the creation of employee-specific product offerings.
- Otherwise securing and facilitating the employee's employment with the group, including rendering to the employee value-added services (such as employee wellness initiatives and catering services), employee administration, training, performance reviews, talent management and other tasks related to the management of employees.
- To share employee / partner / child(ren) personal information for business purposes, e.g., for business travel, events, delivery or collection of gifts, Group assets or packages.
- To share children's details e.g., beneficiaries of pensions on the death of a parent, or if the parent signs the child(ren) up for volunteer project benefits or other promotions or benefits offered by the group from time to time.
- To share close relatives' details – for example emergency contact persons.
- To compile statistics and results from research studies and related programmes.
- To send work-related communications to the employee's mobile device.
- For any other related purposes.

The purposes above indicate the cases where it is mandatory for employees to provide their personal information to enable the processing of:

- The performance of the employment contract to which the employee is party, or to take steps at the request of the prospective employee prior to entering the employment contract.
- Compliance with the legal obligations to which the group is subject.
- The protection of a legitimate interest of the employee.
- The legitimate interests pursued by the group, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

- For a prospective employee: to the group being unable to enter an employment contract with that prospective employee.
- For an employee: to disciplinary sanctions, where applicable, or in extreme cases such refusal may lead to dismissal.

There may be instances where the group will lawfully process personal information for purposes not listed above. Where the provision of personal information does not fall within one of the lawful justifications for processing, separate consent from the employee (which consent may at any moment be withdrawn) will be sought.

3.5. Quality of personal information

FSRN will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate, not misleading, and updated where necessary.

The group human capital functions have provided the self-service channels by means of which employees are required to update personal information if it changes. The onus is on the employee to utilise these channels to update their personal information, when necessary.

For updates of personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

3.6. Security and confidentiality of personal information

All personal information processed by FirstRand Namibia will be held confidential.

FSRN will implement reasonable and appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

3.7. Retention of personal information

Personal information will not be kept by the group for longer than is necessary for the purposes of the processing as set out above, unless a further retention period is required by law, or where FSRN reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and the group.

Other than in the aforementioned instances, the group may request the employee's consent for the further retention of personal information and will state the reasons for such a request.

3.8. The transfer of personal information

Employees' personal information may be shared within the group and with third parties with whom FSRN contracts to process such personal information and pursuant to the instruction of FSRN, under specific terms or terms as set forth in this notice for the purposes mentioned above. A simplified legal entity group structure is available on FirstRand Namibia's website under ownership and legal structure at https://www.firstrandnamibia.com.na/about/ownership-and-legal-structure/.

Provided that FSRN ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of FSRN and in accordance with this notice, FSRN may transfer personal information within the group, to operators (see 3.9 below) or to other third parties based outside Namibia with whom the group has a lawful justification, e.g. parties who signed contracts requiring the other party to adhere to such standards of security and responsible handling in respect of the personal information as adhered to by the Group, regardless of whether the laws of the countries in which such third parties reside provide sufficient safeguards regarding the processing of personal information.

3.9. Use of operators

An operator is a person who processes personal information on behalf of the group in terms of a contract or mandate, without coming under the direct authority of the group.

The group may assign the processing of group employee personal information to an operator, who will process the personal information only with the knowledge or authorisation of FSRN.

The group will contract with the operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by the group.

3.10. Employees' privacy rights

3.10.1 Access to information

The employee has the right to access the personal information which relates to them. Where an employee wishes to request personal information which they do not have a direct right to, but which information is needed to protect a right of the employee, a request must be addressed in accordance with procedure.

Certain personal information relevant to the employee may be accessed through the self-service channels.

3.10.2 Right to correction of personal information

The employee has the right to correct inaccurate personal information which relates to them. The employee can update, and correct certain types of personal information stored on the human capital platform using the self-service channel. For instructions on how to do so, the employee should contact the responsible person in their human capital department.

For updating other types of personal information, the employee should address a request to that effect to the responsible human capital department. Should the group be unable to correct the personal information, it must explain its position in writing to the employee.

Should the group refuse the correction, the employee is entitled to request that a statement be attached to the personal information which indicates that a correction had been sought and was not made.

3.10.3 Right to de-identification/destruction/deletion

The employee is entitled to require the de-identification/ destruction/ deletion of his/ her/ their personal information which is, by reference to the objectives of the processing:

- Inaccurate, irrelevant, excessive, out of date, incomplete or misleading, or which had been obtained unlawfully.
- Legally prohibited from being recorded, communicated, or retained.
- Retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a request to that effect to the responsible human capital department.

The group must delete/remove/destroy this personal information or explain in writing its position regarding the request. Should the group refuse the employee's request for de-identification/ destruction/ deletion, the employee is entitled to request that a statement be attached to the personal information which indicates that a request for de- identification/ destruction/ deletion of personal information had been sought and was not made. The employer's statement should set out the summary for such refusal.

3.10.4 Right to complain

Employees have the right to submit a complaint to the relevant regulator regarding an alleged breach of the conditions for lawful processing of personal information.

An employee can choose to submit a complaint to the group for resolution before submission to the relevant regulator. Any queries or complaints regarding the employee's personal information can be directed to the relevant human capital manager within the group.

3.11. Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice, and for access to information about his, her or their personal information processed within the context of this notice, the employee may contact their data privacy officer, line manager or their human capital department.

The group must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

3.12. Other relevant group policies

- FSRN Ethical Use of Data Framework. This framework aims to ensure effective, efficient, and secure use of the group's information resources, and informs employees of what is deemed acceptable and unacceptable practice. Subject to the terms of this notice, the group will monitor the use of its information resources by employees.
- FSRN privacy governance documents.

FNB LESOTHO EMPLOYEE PRIVACY NOTICE

DOCUMENT CONTROL

Title	FNB Lesotho Employee Privacy Notice		
Author	Compliance		
Document version	1.2		
Version date	February 2024		
Approval	Committee for approval:	Approval date:	Version for approval:
	Risk Committee	……..	….
Date of next review	Upon Regulatory requirement		

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE

Protecting the privacy of personal information of its employees is very important to FNB Lesotho (FNBL). To do so, FNBL follows general principles in accordance with applicable privacy laws and, particularly, the Data Protection Act, FNBL policies and domestic laws applicable in Lesotho pertaining to the subject matter.

FNBL has developed the following FNBL employee privacy notice (**notice**) to help FNBL employees understand how FNBL collects, uses and safeguards their personal information.

FNBL notice includes general information regarding FNBL's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information. FNBL's notice incorporates by reference FNB Lesotho Acceptable Use of Information Resources Policy.

2 SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past and prospective employees (that is, permanent and temporary employees), as well as fixed-term contractors or independent contractors contracted by FNBL.

3 DISCLOSURE INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION.

FNBL will process personal information collected from FNBL employees.

3.1 Data Controller

FNB Lesotho is the data controller.

3.2 Definition of employees' personal information

For the purpose of this notice, and other documents referred to in this notice, personal information means information about an identifiable, living, natural person.

By way of example, an employee's personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

Personal information does not include aggregated or anonymised information where FNBL is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee, which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only. For instance, *"20% of FNBL's employees own or use a laptop computer"* is not personal information.

Personal information, processed by FNBL, regarding its employees (**personal information**) includes the following types of information:

- personal details, including but not limited to, name, address, location information, online identifier, emergency contact details, birth certificate number, employee number or identity number, educational and other qualifications, and curriculum vitae;
- job-related details, e.g. start date, place of work, salary, benefits, absence records;
- financial information, e.g. bank account number;
- performance/evaluation information, e.g. whether an employee performs their job duties in accordance with the relevant requirements.

An employee undertakes to communicate his/her personal information to FNBL when specifically requested by FNBL to do so.

3.3 Definition of employees' special (sensitive) personal information

There are special/sensitive categories of an employee's personal information, which FNBL will only process where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour (**special personal information**).

FNBL processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with FNBL's obligations under relevant pieces of legislation.

FNBL will not retain or process special personal information unless one of the statutory exceptions applies. For example, (where a statutory exception is to obtain consent) specific consent for the processing of biometric personal information may be requested by FNBL.

3.4 Purposes for the processing of personal information

Personal information will be processed by FNBL in the normal course of business of managing employees for various purposes:

- For required banking information in order to process an employee's remuneration.
- To suggest the opening of a bank account on behalf of the employee, in order to secure staff rates.
- To admit the employee to the relevant pension, retirement, or provident funds and/or medical aid providers.
- To comply with FNB Lesotho's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented by FNB Lesotho. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the employee, or prospective employee, including but not limited to politically exposed person (PEP), relevant fraud prevention agencies and services and reference checks where FNBL is not allowed to allow employees to act in certain roles and capacities if they are guilty of fraud or dishonesty. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment.

- To comply with all applicable laws authorising or requiring such processing, including (but not limited to): all employment and labour related laws, laws relating to the safety of employees as work and laws relating to financial crime, fraud, money laundering, KYC, sanctions, combatting of crime and corruption and other corporate laws and their regulations.
- To carry out the specific obligations and duties of FNBL in the field of employment legislation.
- To realise objectives laid down by, or by virtue of, tax or other applicable legislation.
- To properly assess performance under an employment contract.
- To undertake management activities, such as succession planning, talent management, training, work planning, task management, assessment of employee performance, and to control security and access to facilities.
- To market products, goods and services to the employee, the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels, research or statistical purposes and/or the creation of employee-specific product offerings; and/or otherwise securing and facilitating the employee's employment with FNB Lesotho, including rendering to the employee value added services (such as employee wellbeing initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees.
- To share spouse/children personal information for business purposes, e.g. for business travel purposes, events, etc.
- To share children details, e.g. beneficiary of pension on the death of a parent.
- To share close relatives' details – next of kin/emergency contact persons.
- To compile statistics and results from research studies and related programs.
- To process in order to send work-related communications to the employee's mobile device via any of FNBL's platforms and apps.

The purposes above are mandatory for employees to provide their personal information to enable the processing of:

- the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract, or
- compliance with legal obligations to which FNBL is subject, or
- the protection of a legitimate interest of the employee; or
- the legitimate interests pursued by FNBL, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

- for a prospective employee: to FNBL being unable to enter into an employment contract with that prospective employee, and
- for an employee: to disciplinary sanctions, where applicable or, in extreme cases, such refusal may lead to dismissal.

There may be instances where FNBL will lawfully process personal information for purposes not listed above.

Where the provision of personal information is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

3.5 Quality of personal information

FNBL will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate and not misleading, and is updated where necessary.

FNBL's human capital (HR) function have provided the self-service channels, through which employees are required to update personal information if it changes. The onus is on the employee to utilise this channel to update his/her personal information, when necessary.

For updates to personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

3.6 Security and confidentiality of personal information

All personal information processed by FNBL will be held confidentially.

FNBL will take reasonable, appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

3.7 Retention of personal information

Personal information will not be kept by FNBL for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNBL reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and FNBL.

Other than in the aforementioned instances, FNBL may request the employee's consent for the further retention of personal information and will state the reasons for making such a request.

3.8 The transfer of personal information

Employees' personal information may be shared within FNBL and with 3rd parties with whom FNBL contracts to process such personal information and pursuant to the instruction of FNBL, under specific terms or terms as set forth in this notice for the purposes mentioned above.

Provided that FNBL ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of FNBL and in accordance with this notice, FNBL may transfer personal information within FNB Lesotho, operators (see 3.9 below) or other third parties based outside Lesotho and/or outside the particular country where FNBL is incorporated if FNBL has a lawful justification, e.g. a signed a contract requiring the other party to adhere to such standards of security and fair handling in respect of the information as are adhered to by FNBL, regardless of whether the laws of the

countries in which such 3rd parties reside provide sufficient safeguards regarding the processing of personal information.

3.9 Use of operators

An operator is a person who processes personal information on behalf of FNBL in terms of a contract or mandate, without coming under the direct authority of FNBL.

FNBL may assign the processing of FNBL employee personal information to an operator which will process the personal information only with the knowledge or authorisation of FNBL.

FNBL will contract with the operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by FNBL.

3.10 Employees' privacy rights

3.10.1 Access to information

The employee has the right to access the personal information which relates to him/her. Certain personal information relevant to the employee may be accessed through the self-service channel.

3.10.2 Right to correction of personal information

The employee has the right to correct inaccurate personal information which relates to him/her. The employee is able to update, and correct certain types of personal information stored on the human capital platform using the self-service channel. For instructions on how to do so, the employee should contact the responsible person in their human capital department.

For updating other types of personal information, the employee should address a simple request to that effect to the responsible human capital department. Should FNBL be unable to correct the personal information, FNBL must explain its position in writing to the employee.

Should FNBL refuse the correction, the employee is entitled to request that a statement be attached to the personal information, which indicates that a correction has been sought and not made.

3.10.3 Right to de-identification/destruction/deletion

The employee is entitled to require the de-identification/destruction/deletion of his/her/their personal information, which is by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
- legally prohibited from being recorded, communicated or retained; or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a simple request to that effect to the responsible human capital department.

FNBL must delete/remove/destroy this personal information or explain in writing its position regarding the request. Should FNBL refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the personal information, which indicates that a request for removal of personal information has been sought and not made.

3.10.4 Right to complain

Employees have the right to submit a complaint to the information regulator in their country (if such office, or a similar office, had been created) regarding an alleged breach of the conditions for lawful processing of personal information.

An employee can choose to submit complaints to FNBL for resolution before submission to the information regulator. Any queries or complaints regarding the employee's personal information can be directed to the respective human capital manager within the FNBL.

3.11 Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice and for access to information about his or her personal information processed within the context of this notice, (e.g. employee discloses his HIV status to his line manager, who then communicates this to the entire office) the employee may contact their data privacy officer, line manager or their human capital department.

FNBL must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

3.12 Reference to other FNBL policies

- FNB Lesotho Acceptable Use of Information Resources Policy.
- FNB Lesotho Internal Privacy Policy.
- FNB Lesotho Data Privacy Framework.

-END-

POLÍTICA DE PRIVACIDADE DO COLABORADOR DO FNB

DOCUMENTO DE CONTROLO

Título	Política de Privacidade do Colaborador do FNB		
Autor	Operações		
Versão do Documento	0.5		
Data	June 2020		
Aprovação	Comité de aprovação:	Data de aprovação:	Versão para aprovação:
	Comité de privacidade e protecção de dados	June 2020	0.5
Data da próxima revisão	Abril de 2021. As alterações respeitantes à Política entrarão em vigor quando os colaboradores e/ou os representantes dos colaboradores tiverem sido informados/consultados sobre/consentido essas alterações, de acordo com os requisitos legais aplicáveis.		

TABELA DE CONTEÚDOS

1. CONTEXTO E PROPÓSITO

A protecção da privacidade de informação pessoal dos seus colaboradores é muito importante para o FNB Moçambique (FNB). Para o efeito, o FNB segue princípios gerais de acordo com as leis de privacidade aplicáveis e, particularmente, a Convenção da União Africana para a Privacidade de Dados e Segurança Cibernética (Convenção).

O FNB desenvolveu a seguinte política de privacidade (aviso) para auxiliar os colaboradores do FNB a compreenderem como o FNB recolhe, usa e salvaguarda a sua informação pessoal.

A política do FNB inclui informação geral sobre o tratamento de informação pessoal dos colaboradores e os direitos e responsabilidades dos colaboradores por parte do FNB no que diz respeito à sua informação pessoal. A política do FNB incorpora por referência a política de uso aceitável de recursos de informação do FNB.

2. ÂMBITO

Esta política aplica-se a todos os colaboradores, definidos para propósitos do presente documento como colaboradores efectivos, antigos e potenciais (ou seja, colaboradores permanentes e temporários), bem como aos contratados a termo certo ou aos contratados independentes contratados pelo FNB.

3. DIVULGAÇÃO DE INFORMAÇÃO RELACIONADA COM OS DIREITOS E RESPONSABILIDADES DOS COLABORADORES NO QUE DIZ RESPEITO À SUA INFORMAÇÃO PESSOAL.

O FNB processará a informação pessoal recolhida dos colaboradores.

3.1 Parte responsável

FNB MOÇAMBIQUE, S.A. (FNB), uma sociedade constituída sob a forma de instituição de crédito, com sede em Maputo, na Avenida 25 de Setembro, n.º 420, Edifício JAT I, 1º andar, Sala 8, Cidade de Maputo, matriculada na Conservatória do Registo das Entidades Legais sob o número 12.540, sheets 162, a folhas 162 do Livro C - 30, titular do NUIT 400076391. Esta empresa é a parte responsável.

3.2 Definição de informação pessoal dos colaboradores

Para efeitos da presente política, e de outros documentos referidos na presente política, informação pessoal significa informação sobre uma pessoa singular, viva e identificável.

A título de exemplo, a informação pessoal de um colaborador pode incluir a raça, sexo, número de identificação, número do colaborador, endereço residencial, número de telefone, data de nascimento, estado civil, deficiência, informação biométrica e correspondência enviada ou recebida por um colaborador que seja implícita ou explicitamente privada ou confidencial.

A informação pessoal não inclui informação agregada ou anónima quando o FNB é incapaz de identificar um colaborador. A informação agregada ou anónima inclui qualquer informação sobre um colaborador, que pode ser incluída como parte de uma declaração sobre um grupo de colaboradores ou um gráfico ou gráfico circular apresentando características apenas como parte de um grupo de colaboradores. Por exemplo, "20% dos colaboradores do FNB possuem ou utilizam um computador portátil" não é informação pessoal.

A informação pessoal, processada pelo FNB, relativa aos colaboradores do FNB (**informação pessoal**) inclui os seguintes tipos de informação:

- dados pessoais, incluindo mas não limitados a, nome, morada, informações de localização, identificador online, dados de contacto de emergência, número da certidão de nascimento, número do colaborador ou número de identidade, habilitações académicas e outras qualificações, e curriculum vitae;
- detalhes relacionados com o trabalho, por exemplo, data de início, local de trabalho, salário, benefícios, registos de ausência;
- informações financeiras, p. ex. número de conta bancária;
- informação sobre desempenho/avaliação, p. ex. se um colaborador desempenha as suas funções de acordo com os requisitos relevantes.

Um colaborador compromete-se a comunicar a sua informação pessoal ao FNB quando especificamente solicitado pelo FNB neste sentido.

3.3 Definição de informação pessoal especial dos colaboradores

Existem categorias especiais de informação pessoal de um colaborador, que o FNB só processará quando um conjunto elevado de requisitos for cumprido. Estas categorias especiais são informações que revelam crenças religiosas ou filosóficas, raça ou origem étnica, filiação sindical, persuasão política, saúde ou vida sexual, informações biométricas, e certas informações relativas a infracções e comportamentos criminosos (**informações pessoais especiais**).

O FNB processa informações médicas e de saúde com o consentimento do colaborador para efeitos de seguros e acordos de assistência médica celebrados em nome do colaborador e em seu benefício, e a fim de cumprir as obrigações do FNB ao abrigo das leis e regulamentos aplicáveis.

O FNB não irá reter ou processar informação pessoal especial, a menos que se aplique uma das excepções legais. Por exemplo, (quando uma excepção legal for a obtenção de consentimento) o consentimento específico para o processamento de informação pessoal biométrica pode ser solicitado pelo FNB.

3.4 Propósitos do processamento de informação pessoal

A informação pessoal será processada pelo FNB no decurso normal do negócio da gestão de colaboradores para vários fins:

- Para informação bancária necessária a fim de processar a remuneração de um colaborador.
- Para sugerir a abertura de uma conta bancária em nome do colaborador, a fim de garantir as taxas do pessoal.
- Para admitir o colaborador na Segurança Social.
- Para cumprir as obrigações do FNB em matéria de combate ao branqueamento de capitais, financiamento do terrorismo, detecção de fraude e corrupção, bem como os processos de gestão de risco implementados. Isto incluirá a realização de controlos criminais, de crédito, de referência, de sanções, anti-suborno e outros controlos de referência relacionados com o colaborador, ou potencial colaborador. Tais verificações podem ser conduzidas de forma contínua durante todo o período de emprego e podem incluir auditorias ao estilo de vida, bem como relatórios sobre a conduta dos colaboradores, quando exigido por lei, aos organismos competentes após a cessação do emprego.
- Para cumprir todas as leis aplicáveis que autorizem ou exijam tal processamento.
- Cumprir as obrigações e deveres específicos do FNB no domínio da legislação laboral.
- Cumprir os objectivos estabelecidos por, ou em virtude de, legislação fiscal ou outra legislação aplicável.
- Avaliar devidamente o desempenho no âmbito de um contrato de trabalho.
- Realizar actividades de gestão, tais como planeamento sucessório, gestão de talentos, formação, planeamento do trabalho, gestão de tarefas, avaliação do desempenho dos colaboradores, e controlar a segurança e o acesso às instalações.
- Comercializar produtos, bens e serviços ao colaborador, o envolvimento do colaborador em projectos-piloto relacionados com produtos, serviços, plataformas, bens e canais novos ou actualizados, fins de investigação ou estatísticos e/ou a criação de ofertas de produtos específicos para o colaborador; e/ou assegurar e facilitar o emprego do colaborador no FNB, incluindo a prestação ao colaborador de serviços de valor acrescentado (tais como iniciativas de bem-estar do colaborador e serviços de restauração), administração do colaborador, formação, análises de desempenho, gestão de talentos e outras razões relacionadas com a gestão dos colaboradores.
- Partilhar informações pessoais do cônjuge/filhos para fins profissionais, por exemplo, para viagens de negócios, eventos, etc.
- Partilhar os dados dos filhos, por exemplo, beneficiário de pensão por morte de um dos pais.
- Para partilhar dados de familiares próximos - parentes próximos/pessoas de contacto em caso de emergência.

- Para compilar estatísticas e resultados de estudos de investigação e programas relacionados.
- Processar a fim de enviar comunicações relacionadas com o trabalho para o dispositivo móvel do colaborador através de qualquer uma das plataformas do grupo, incluindo as aplicações do RMB, FNB e WesBank.
- Os propósitos acima referidos são obrigatórios para que os colaboradores forneçam as suas informações pessoais para permitir o processamento das mesmas:
- a execução do contrato de trabalho em que o trabalhador é parte ou para tomar medidas a pedido do potencial colaborador antes de celebrar o contrato de trabalho, ou
- o cumprimento das obrigações legais a que ao FNB está sujeito, ou
- a protecção de um interesse legítimo do colaborador; ou
- os interesses legítimos seguidos pelo FNB, ou pelo terceiro a quem as informações pessoais são divulgadas para os fins acima referidos.

Se um colaborador se recusar a fornecer as informações pessoais necessárias para estes fins, isto pode conduzir a uma situação em que o colaborador se recusa a fornecer as informações pessoais solicitadas:

- para um potencial colaborador: que o FNB não possa celebrar um contrato de trabalho com esse potencial colaborador, e
- para um colaborador: no caso do FNB não poder prestar serviços e/ou privilégios ao colaborador e aos seus dependentes, não cumprir ordens/instruções por exigência ou interesse ou, em casos extremos, essa recusa pode levar à rescisão do contrato se a extensão dessa recusa se tornar materialmente adversa a manutenção da relação.

Pode haver casos em que o FNB processará legalmente informações pessoais para fins não indicados acima.

Quando o fornecimento de informação pessoal não for para um processo legal, será solicitado um consentimento separado e escrito do colaborador (que pode ser anulado a qualquer momento).

3.5 Qualidade de informação pessoal

O FNB tomará medidas razoáveis e praticáveis para assegurar que as informações pessoais dos colaboradores sejam completas, precisas e não enganosas, e que sejam actualizadas sempre que necessário.

As funções do capital humano do FNB forneceram os canais de auto-serviço, através dos quais os colaboradores são obrigados a actualizar a informação pessoal em caso de alteração. Compete ao colaborador utilizar este canal para actualizar a sua informação pessoal, quando necessário.

Para actualizações de informações pessoais que não são possíveis através do canal de auto-serviço, os colaboradores são obrigados a dirigir o respectivo pedido ao departamento de capital humano responsável.

3.6 Segurança e confidencialidade de informação pessoal

Toda a informação pessoal processada pelo FNB será mantida confidencialmente.

O FNB tomará medidas técnicas e organizacionais razoáveis e apropriadas para manter a informação pessoal segura, de acordo com as suas políticas e procedimentos sobre segurança da informação, e em conformidade com qualquer legislação aplicável.

3.7 Retenção de informação pessoal

A informação pessoal não será mantida pelo FNB por um período superior ao necessário para os fins do processamento acima referido, a menos que um período de retenção adicional seja exigido por lei, ou quando o FNB exigir razoavelmente um período de retenção adicional para um fim legal relacionado com as suas funções ou actividades, ou quando um período de retenção adicional for exigido por um contrato entre o colaborador e o FNB.

Excepto nos casos acima mencionados, o FNB pode solicitar o consentimento do colaborador para a retenção adicional de informação pessoal e indicará as razões do pedido.

3.8 A transferência de informação pessoal

A informação pessoal dos colaboradores pode ser partilhada pelo FNB com terceiros com quem o FNB contrata para processar tal informação pessoal e de acordo com as instruções do FNB, em termos ou condições específicas, conforme estabelecido na presente política para os fins acima mencionados. Uma estrutura de entidade jurídica simplificada para o grupo FirstRand pode ser consultada através do seguinte link https://www.firstrand.co.za/the-group/ownership-and-legal-structure/.

Desde que o FNB assegure salvaguardas adequadas e/ou celebre um contrato para terceiros para processar informação pessoal para os fins acima mencionados, de acordo com as instruções do FNB e em conformidade a presente política, o FNB pode transferir informação pessoal ao nível do grupo, operadores (ver 3.9 abaixo) ou outros terceiros sediados fora de Moçambique com os quais o FNB tenha uma justificação legal, por exemplo: um contrato assinado exigindo que a outra parte adira às normas de segurança e tratamento justo da informação que são seguidas pelo FNB, independentemente de as leis dos países em que tais terceiros residem fornecerem garantias suficientes no que diz respeito ao processamento de informação pessoal.

3.9 Uso de operadores

Um operador é uma pessoa que processa informações pessoais em nome do FNB nos termos de um contrato ou mandato, sem estar sob a autoridade directa do FNB.

O FNB pode atribuir o processamento da informação pessoal dos colaboradores do FNB a um operador que só processará a informação pessoal com o conhecimento ou autorização do FNB.

O FNB fará um contrato com o operador para assegurar que as informações pessoais são mantidas confidenciais, e sujeitas às normas de segurança e tratamento justo no que diz respeito às informações, tal como são cumpridas pelo FNB.

3.10 Direitos de privacidade dos colaboradores

3.10.1 Acesso à informação

O colaborador tem o direito de aceder às informações pessoais que lhe dizem respeito. Quando um colaborador deseja solicitar informação pessoal, à qual não tem direito directo, a qual é necessária para proteger um direito dos colaboradores, deverá ser apresentado um pedido aos tribunais judiciais.

3.10.2 Direito à correcção de informação pessoal

O colaborador tem o direito de corrigir informações pessoais incorrectas que lhe digam respeito. O colaborador é capaz de actualizar, e corrigir determinados tipos de informação pessoal armazenadas na plataforma de capital humano, utilizando o canal de auto-serviço. Para instruções sobre como o fazer, o colaborador deve contactar a pessoa responsável do departamento de capital humano.
Para actualizar outros tipos de informação pessoal, o colaborador deve apresentar um simples pedido para o efeito ao departamento de capital humano responsável. Caso o FNB não consiga corrigir a informação pessoal, o FNB deve explicar a sua posição por escrito ao colaborador.

Se o FNB recusar o pedido de correcção, o colaborador tem o direito de solicitar que seja anexada uma declaração às informações pessoais, o que indica que foi solicitada uma correcção e não efectuada.

3.10.3 Direito à anulação de identificação/destruição/remoção

O colaborador goza do direito de exigir a anulação de identificação/destruição/remoção da sua informação pessoal, que é por referência aos objectivos do processamento:

- incorrecta, irrelevante, excessiva, desactualizada, incompleta, enganosa ou obtida de forma ilegal;
- legalmente proibido de ser registado, comunicado ou retido; ou
- retidos para além de um período razoável após o termo do contrato de trabalho entre as partes.

Para o efeito, o colaborador deve apresentar um simples pedido nesse sentido ao departamento de capital humano responsável.

O FNB deve apagar/remover/destruir esta informação pessoal ou explicar por escrito a sua posição relativamente ao pedido. Caso o FNB recuse o pedido do colaborador para a anulação de identificação/destruição/remoção, o colaborador goza do direito de solicitar que seja anexada uma declaração às informações pessoais, que indique que foi solicitado um pedido de remoção de informações pessoais e que não foi feito.

3.10.4 Direito de reclamar

Os colaboradores gozam do direito de apresentar uma reclamação à Autoridade Nacional de Protecção de Dados ou outra autoridade competente relativamente a uma alegada violação das condições de tratamento legal de informações pessoais, conforme estabelecido na Convenção e outras leis e regulamentos aplicáveis.

Um colaborador pode optar por apresentar reclamações ao FNB para resolução antes de as submeter à Autoridade Nacional de Privacidade de Dados . Quaisquer questões ou reclamações relativas às informações pessoais do colaborador podem ser encaminhadas para o respectivo gestor do capital humano ao nível do FNB.

3.11 Pessoas de contacto

Para quaisquer questões, perguntas ou reclamações relativas à aplicação da presente política e para acesso a informações sobre as suas informações pessoais processadas no contexto desta política, (por exemplo, o colaborador revela o seu estado de seropositividade ao seu superior hierárquico, que depois o comunica a todo o pessoal) o colaborador pode contactar o seu responsável pela privacidade dos dados, o seu superior hierárquico ou o seu departamento de capital humano.

O FNB deve registar por escrito qualquer reclamação do colaborador ou de terceiros relacionada com a divulgação de informações pessoais do colaborador, e responder a essa reclamação, mantendo um registo da referida resposta.

3.12 Referência sobre outras políticas do FNB

- Política de uso aceitável de recursos de informação do FNB:
  https://FNBgroup.sharepoint.com/sites/FCCERM/ITGovernance/SitePages/Policies.aspx
  A política de uso aceitável dos recursos de informação da FNB visa assegurar uma utilização eficaz, eficiente e segura dos recursos de informação do FNB e informar os colaboradores do que é considerado uma prática aceitável e inaceitável. Sujeito aos termos desta política, o FNB deverá monitorar o uso dos seus recursos de informação dos seus colaboradores. A presente política também contém requisitos e orientações respeitantes ao tratamento de informações pessoais dos clientes.
- Política de Privacidade Interna do FNB.
- Estrutura de Privacidade do FNB

-FIM-

FNB EMPLOYEE PRIVACY NOTICE

DOCUMENT CONTROL

POLICY LEVEL:	FNBM
EFFECTIVE DATE:	
NUMBER OF PAGES:	9
DATE	
APPROVED BY:	Head of Department and noted at EXCO
Document Owner	Name: Melba Jorge Designation: Head of Human Resources Physical Address: 420, 25 de Setembro, JATI, 1st Floor Tel: +258 21 35 5905 e-mail: Melba.jorge@fnb.co.mz
VERSION NUMBER:	1.0

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE

Protecting the privacy of personal information of its employees is very important to FNB Moçambique S.A. (FNB). To do so, FNB follows general principles in accordance with applicable privacy laws and, particularly, the African Union Convention for Data Privacy and Cybersecurity (Convention).

FNB has developed the following FNB employee privacy notice (notice) to help employees understand how FNB collects, uses and safeguards their personal information.

FNB's notice includes general information regarding FNB's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information. FNB's notice incorporates by reference FNB's acceptable use of information resources policy.

2. SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past and prospective employee (that is, permanent and temporary employees), as well as fixed-term contractors or independent contractors contracted by the FNB.

3. DISCLOSURE INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION.

FNB will process personal information collected from employees.

3.1 Responsible party

FNB MOÇAMBIQUE, S.A. (FNB), a joint stock company, with headquarter at September 25 Avenue, no. 420, JAT Building I, 1st floor, Room 8, in Maputo City, registered at legal Entities Register under the number 12,540, sheets 162, of Book C-30, holder of the Tax Identification Number 400076391, This company is the responsible party.

3.2 Definition of employees' personal information

For the purpose of this notice, and other documents referred to in this notice, personal information means information about an identifiable, living, natural person.

By way of example, an employee's personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

Personal information does not include aggregated or anonymised information where FNB is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee, which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only. For instance, "20% of FNB's employees own or use a laptop computer" is not personal information.

Personal information, processed by FNB, regarding FNB employees (**personal information**) includes the following types of information:

- personal details, including but not limited to, name, address, location information, online identifier, emergency contact details, birth certificate number, employee number or identity number, educational and other qualifications, and curriculum vitae;
- job-related details, e.g. start date, place of work, salary, benefits, absence records;
- financial information, e.g. bank account number;
- performance/evaluation information, e.g. whether an employee performs their job duties in accordance with the relevant requirements.

An employee undertakes to communicate his/her personal information to FNB when specifically requested by FNB to do so.

3.3 Definition of employees' special personal information

There are special categories of an employee's personal information, which FNB will only process where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour (**special personal information**).

FNB processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with FNB's obligations under the applicable laws and regulations.

FNB will not retain or process special personal information unless one of the statutory exceptions applies. For example, (where a statutory exception is to obtain consent) specific consent for the processing of biometric personal information may be requested by FNB.

3.4 Purposes for the processing of personal information

Personal information will be processed by FNB in the normal course of business of managing employees for various purposes:

- For required banking information in order to process an employee's remuneration.
- To suggest the opening of a bank account on behalf of the employee, in order to secure staff rates.
- To admit the employee to the Social Insurance.
- To comply with the FNB's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the employee, or prospective employee. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment.
- To comply with all applicable laws authorising or requiring such processing.
- To carry out the specific obligations and duties of FNB in the field of employment legislation.
- To realise objectives laid down by, or by virtue of, tax or other applicable legislation.
- To properly assess performance under an employment contract.
- To undertake management activities, such as succession planning, talent management, training, work planning, task management, assessment of employee performance, and to control security and access to facilities.
- To market products, goods and services to the employee, the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels, research or statistical purposes and/or the creation of employee-specific product offerings; and/or otherwise securing and facilitating the employee's employment with the FNB, including rendering to the employee value added services (such as employee wellbeing initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees.
- To share spouse/children personal information for business purposes, e.g. for business travel purposes, events, etc.
- To share children details, e.g. beneficiary of pension on the death of a parent.
- To share close relatives' details – next of kin/emergency contact persons.
- To compile statistics and results from research studies and related programs.
- To process in order to send work-related communications to the employee's mobile device via any of the group's platforms including the RMB, FNB and WesBank apps.
- The purposes above are mandatory for employees to provide their personal information to enable the processing of:
- the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract, or
- compliance with legal obligations to which FNB is subject, or
- the protection of a legitimate interest of the employee; or

- the legitimate interests pursued by FNB, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

- for a prospective employee: to FNB being unable to enter into an employment contract with that prospective employee, and
- for an employee: to FNB being unable to provide services and/or privileges to the employee and his dependents, not fulfil orders/instructions by his demand or interest or, in extreme cases, such refusal may lead to terminate the contract if the extent of such refusal become materially adverse the maintenance of the relationship.

There may be instances where FNB will lawfully process personal information for purposes not listed above.

Where the provision of personal information is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

3.5 Quality of personal information

FNB will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate and not misleading, and is updated where necessary.

The FNB's human capital functions have provided the self-service channels, through which employees are required to update personal information if it changes. The onus is on the employee to utilise this channel to update his/her personal information, when necessary.

For updates to personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

3.6 Security and confidentiality of personal information

All personal information processed by FNB will be held confidentially.

FNB will take reasonable, appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

3.7 Retention of personal information

Personal information will not be kept by FNB for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNB reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and FNB.

Other than in the instances, FNB may request the employee's consent for the further retention of personal information and will state the reasons for making such a request.

3.8 The transfer of personal information

Employees' personal information may be shared by FNB with third parties with whom FNB contracts to process such personal information and pursuant to the instruction of FNB, under specific terms or terms as set forth in this notice for the purposes mentioned above.

Provided that FNB ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of FNB and in accordance with this notice, FNB may transfer personal information within the group, operators (see 0 below) or other third parties based outside Mozambique with whom FNB has a lawful justification, e.g. a signed a contract requiring the other party to adhere to such standards of security and fair handling in respect of the information as are adhered to by FNB, regardless of whether the laws of the countries in which such third parties reside provide sufficient safeguards regarding the processing of personal information.

3.9 Use of operators

An operator is a person who processes personal information on behalf of FNB in terms of a contract or mandate, without coming under the direct authority of FNB.

FNB may assign the processing of FNB employee personal information to an operator which will process the personal information only with the knowledge or authorisation of FNB.

FNB will contract with the operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by FNB.

3.10 Employees' privacy rights

3.10.1 Access to information

The employee has the right to access the personal information which relates to him/her. Where an employee wishes to request personal information, which they do not have a direct right to, but which information is needed to protect a right of the employees, a request must be addressed judicial courts.

3.10.2 Right to correction of personal information

The employee has the right to correct inaccurate personal information which relates to him/her. The employee can update, and correct certain types of personal information stored on the human capital platform using the

self-service channel. For instructions on how to do so, the employee should contact the responsible person in their human capital department.
For updating other types of personal information, the employee should address a simple request to that effect to the responsible human capital department. Should FNB be unable to correct the personal information, FNB must explain its position in writing to the employee.

Should FNB refuse the correction, the employee is entitled to request that a statement be attached to the personal information, which indicates that a correction has been sought and not made.

3.10.3 Right to de-identification/destruction/deletion

The employee is entitled to require the de-identification/destruction/deletion of his/her/their personal information, which is by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
- legally prohibited from being recorded, communicated or retained; or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a simple request to that effect to the responsible human capital department.

FNB must delete/remove/destroy this personal information or explain in writing its position regarding the request. Should FNB refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the personal information, which indicates that a request for removal of personal information has been sought and not made.

3.10.4 Right to complain

Employees have the right to submit a complaint to the Data Privacy National Authority or other competent authority regarding an alleged breach of the conditions for lawful processing of personal information as set out in Convention and other applicable laws and regulation.

An employee can choose to submit complaints to FNB for resolution before submission to the Data Privacy National Authority. Any queries or complaints regarding the employee's personal information can be directed to the respective human capital manager within the FNB.

3.11 Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice and for access to information about his or her personal information processed within the context of this notice, (e.g. employee discloses his HIV status to his line manager, who then communicates this to the entire office) the employee may contact their data privacy officer, line manager or their human capital department.

FNB must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

3.12 Reference to other FNB policies

- FNB acceptable use of information resources policy:

  The FNB acceptable use of information resources policy aims to ensure effective, efficient and secure use of FNB's information resources and informs employees of what is deemed acceptable and unacceptable practice. Subject to the terms of this notice, FNB will monitor the use of its information resources by employees. This notice also contains requirements and guidelines for dealing with the personal information of clients.
- FNB internal privacy policy.
- FNB privacy framework.

-END-

RMB INTERNATIONAL (MAURITIUS) LIMITED ("RMBIM")

EMPLOYEE PRIVACY NOTICE

DOCUMENT CONTROL

Title	RMBIM Employee Privacy Notice		
Author	Regulatory and Conduct Risk Management / RMBIM Compliance Officer		
Document version	1.0		
Version date	23 April 2021		
Approval	Committee for Approval:	Approval date:	Version for approval:
	RMBIM Management Committee	July 2023	3.0
Date of review	June 2023		
Date of next review	June 2024		

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE

Protecting the privacy of personal information (PI) of its employees is very important to RMBIM. To do so, RMBIM follows general principles in accordance with applicable privacy laws and, particularly, the Data Protection Act 2017.

RMBIM has developed the following RMBIM Employee Privacy Notice (the "Notice") to help its employees understand how RMBIM and the broader FirstRand Group collects, uses and safeguards their PI.

This Notice includes general information regarding RMBIM's treatment of employees' PI and employees' rights and responsibilities in respect of their PI.

2. SCOPE

3. THIS NOTICE APPLIES TO ALL EMPLOYEES, DEFINED FOR PURPOSES THROUGHOUT THIS DOCUMENT AS CURRENT, PAST AND PROSPECTIVE PERMANENT EMPLOYEES. DISCLOSURE OF INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PI.

3.1 RMBIM - Responsible Parties

RMBIM will process PI collected from its employees and also make it available to the following Responsible Parties for processing:

- FirstRand Bank Limited (payroll and human capital)
- Rand Merchant Bank as a division of FirstRand Bank Limited
- Adansonia Management Services Limited (company secretary & payroll)
- Swan General Ltd (pension and medical scheme)

3.2 Definition of Employees' PI

For the purpose of this Notice, and other documents referred to in this Notice, PI means information about an identifiable, living, and natural person.

By way of examples, an employee's PI may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

PI does not include aggregated or anonymised information where RMBIM and/or FirstRand is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only.

PI, collected and processed by RMBIM, regarding RMBIM employees includes the following types of information:

- personal details, but is not limited to, e.g., name, address, location information, online identifier, emergency contact details, birth certificate number, employee number or identity number, educational/ other qualifications, and curriculum vitae;
- job-related details: e.g., start date, place of work, salary, benefits, absence records;
- financial information: e.g., bank account number;
- performance/ evaluation information: e.g., whether an employee performs job duties in accordance with the relevant requirements.

An employee undertakes to communicate his/her PI to RMBIM when specifically requested by RMBIM to do so.

3.3 Definition of Employees' Special Personal Information (SPI)

There are special categories of an employee's PI which RMBIM will only process or make available to Responsible Parties for processing where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour, which is referred to as SPI.

RMBIM processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with RMBIM's obligations under the Occupational Health and Safety Act 2005.

RMBIM will not retain or process SPI unless one of the statutory exceptions applies. For example, (where a statutory exception is to obtain consent) specific consent for the processing of biometric PI may be requested by RMBIM.

3.4 Purposes for the Processing of PI

PI will be processed by RMBIM and/or made available to Responsible Parties for processing in the normal course of business of managing employees for various purposes:

- Requires banking information in order to process an employee's remuneration;
- Admitting the Employee to RMBIM's pension fund with Swan Pensions Ltd;
- Admitting the Employee to the medical aid scheme with Swan Insurance Ltd;
- Complying with the Group's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented by the Group. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the Employee, or prospective Employee, including but not limited to Register of Employees' Dishonesty System (REDS), Politically Exposed Person (PEP), South African Fraud Prevention Services (Shamwari), Life Offices' Association (LOA) and Financial Advisory and Intermediary Service Act (FAIS) reference checks. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment;
- Complying with all applicable laws authorising or requiring such processing, including **(but not limited to)**: the Worker's Rights Act 2019, the Occupational Health and Safety Act 2005, the

Financial Intelligence Anti Money Laundering Act 2002, the Prevention of Corruption Act 2002, and the Companies Act 2001;
- Carrying out the specific obligations and duties of RMBIM 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;
- Securing and facilitating the employee's employment with the Group, including rendering to the employee value added services (such as employee wellness initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees;
- Sharing spouse/ children PI for business purposes. E.g., for business travelling purposes, events etc.;
- Sharing of children details for e.g., beneficiary of pension, on the death of a parent.;
- Sharing of close relative's details – next of kin/emergency contact persons;
- Compile statistics and results from research studies and related programs; and
- Processing in order to send work related communications to the employee's mobile device via any of FirstRand's platforms including the RMB and FNB apps.

The above-mentioned purposes require employees to provide their PI to enable the processing of:
- the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract; or
- compliance with legal obligations to which RMBIM is subject; or
- the protection of a legitimate interest of the employee; or
- the legitimate interests pursued by RMBIM, or by the third party to whom the PI is disclosed for the above purposes.

If an employee refuses to provide the required PI for these purposes, this may lead:
- for a prospective employee: to them being unable to enter into an employment contract with RMBIM; and
- for an employee: to disciplinary sanctions, where applicable, or in extreme cases such refusal may lead to dismissal.

There may be instances where RMBIM will lawfully process PI for purposes not listed above. Where the provision of PI is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

3.5 Quality of PI

RMBIM will take reasonable and practicable steps to ensure that the PI of employees is complete, accurate and not misleading, and is updated at all times. It is the responsibility of employees to update their PI in case of change.

3.6 Security and Confidentiality of PI

All PI processed by RMBIM and FirstRand will be held confidentially.

RMBIM and FirstRand will take reasonable, appropriate technical and organisational measures to keep PI secure in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

3.7 Retention of PI

PI will not be kept by RMBIM and FirstRand for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where RMBIM and FirstRand reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and FirstRand.

Other than in the aforementioned instances, RMBIM and FirstRand may request the employee's consent for the further retention of PI and will state the reasons for making such a request.

3.8 The Transfer of PI

Employees' PI may be shared within the FirstRand Group and with third parties with whom RMBIM and FirstRand contracts to process such PI and pursuant to the instructions of RMBIM and FirstRand, under specific terms or terms as set forth in this Notice for the purposes mentioned above.

Provided that RMBIM and FirstRand ensures adequate safeguards and/or enters into a contract for third parties to process PI for the purposes mentioned above, pursuant to the instruction of RMBIM and FirstRand and in accordance with this Notice, RMBIM and FirstRand may transfer PI within the Group, or other third parties with whom RMBIM and FirstRand have a lawful justification e.g. a signed contract requiring the other party to adhere to such standards of security and fair handling in respect of the information as are adhered to by RMBIM and FirstRand, regardless of whether the laws of the countries in which such third parties reside provide sufficient safeguards regarding the processing of PI.

3.9 Employees' Privacy Rights

3.9.1 Access to Information

The employee has the right to access the PI which relates to him or her. Where an employee wishes to request PI, which they do not have a direct right to, but which information is needed to protect a right of the employees, a request must be addressed in accordance with the procedure referred to in RMBIM's Data Protection Manual prepared in accordance with the Data Protection Act 2017. This manual may be obtained on Helium.

3.9.2 Right to Correction of PI

The employee has the right to correct inaccurate PI which relates to him or her.

For updating other types of PI, the employee should address a simple request to his or her line manager or the responsible HR Department. Should RMBIM be unable to correct the PI, RMBIM must explain its position in writing to the employee.

Should RMBIM refuse the correction, the employee is entitled to request that a statement be attached to the PI which indicates that a correction has been sought and not made.

3.9.3 Right to de-identification/ destruction/ deletion

The employee is entitled to require the de-identification/ destruction/ deletion of his/her/their PI which is, by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully;
- legally prohibited from being recorded, communicated, or retained; or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a simple request to that effect to his/her line manager or the responsible HR Department.

RMBIM must delete/remove/destroy this PI or explain in writing its position regarding the request. Should RMBIM refuse the employee's request for de-identification/ destruction/ deletion, the employee is entitled to request that a statement be attached to the PI which indicates that a request for removal of PI has been sought and not made.

3.9.4 Right to complain

Employees have the right to submit a complaint to the Data Protection Office (DPO) regarding an alleged breach of the conditions for lawful processing of PI as set out in DPA.

An employee can choose to submit complaints to RMBIM for resolution before submission to the DPO. Any queries or complaints regarding the employees PI can be directed to the RMBIM Data Protection Officer.

3.10 Contact Persons

For any PI protection issues, questions or complaints concerning the application of the Notice and for access to information about his or her PI processed within the context of this Notice, the employee may contact RMBIM’s Data Protection Officer or his/her line manager.

RMBIM must record in writing any employee or third-party complaint relating to the disclosure of employee PI, and respond to that complaint, keeping a record of such response.

First National Bank

First National Bank Zambia Limited
Employee Privacy Notice

Policy information	Responsibility	
Policy Owner:	*Designation:* *Physical Address:*	Chief Operating Officer Plot No. 22768 Acacia Business Park, Thabo Mbeki Road, Lusaka
Approval:	*Committee*	*Approval/ Review Date*
	EXCO	
Date of next review:	February 2025/Annually	
Document version no:	4	

DOCUMENT VERSION CONTROL				
Document Location Primary		http://africansubs/zambia/rac/Framework%20Documentation/Forms/AllItems.aspx		
File Name		FNBZ Employee Privacy Notice		
Author(s)		Chief Operating Officer		
Date approved		Date for review	Reviewer (s)	Approving Committee
			Relevant Management Subcommittee	EXCO
Version	Status	Date	Comments	
4	Reviewed	February 2024	Policy Review	

TABLE OF CONTENTS

1 BACKGROUND AND PURPOSE

Protecting the privacy of personal information of its employees is very important to FNB Zambia Limited (FNBZ). To do so, FNBZ follows general principles in accordance with applicable privacy laws and, particularly, the Data Protection Act of 2021, FNBZ's policies in this regard and equivalent domestic laws applicable to the subject matter.

FNBZ has developed the employee privacy notice to help employees understand how FNBZ collects, uses and safeguards their personal information.

FNBZ's notice includes general information regarding FNBZ's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information. FNBZ's notice incorporates by reference FNB's acceptable use of information resources policy.

2 SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past and prospective employee (that is, permanent and temporary employees) as well as fixed-term contractors or independent contractors contracted by FNBZ.

3 DISCLOSURE OF INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION.

FNBZ will process personal information collected from employees.

3.1 Responsible parties in FNB Zambia

FNBZ Ltd, means First National Bank Zambia Limited.

3.2 Definition of employees' personal information

For the purpose of this notice, and other documents referred to in this notice, personal information means information about an identifiable and living natural person.

By way of example, an employee's personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

Personal information does not include aggregated or anonymised information where FNBZ is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee, which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only. For instance, *"20% of FNBZ's employees own or use a laptop computer"* is not personal information.

Personal information, processed by FNBZ, regarding FNBZ employees (**personal information**) includes the following types of information:

- your marital status (like married, single, divorced).
- your national origin.
- your age.
- your language, birth, education,
- your financial history (like your income or your buying, investing and banking behaviour based on, amongst others, account transactions).
- your identifying number (like an account number, identity number or passport number).
- your e-mail address, physical address (like residential address, work address or your physical location), telephone number.
- your online identifiers, social media profiles.
- your biometric information (like fingerprints, your signature or voice).
- your race, gender, sex, pregnancy, ethnic origin, social origin, colour, sexual orientation.
- your physical health, mental health, well-being, disability, religion; belief, conscience, culture.
- your medical history (like your HIV / AIDS status), criminal history, employment history.
- your personal views, preferences and opinions.
- your confidential correspondence.
- another's views or opinions about you and your name also constitute your personal information.

Personal information includes special personal information, as explained below.

An employee undertakes to communicate his/her personal information to FNBZ when specifically requested by FNBZ to do so.

3.3 Definition of employees' special personal information

There are special categories of an employee's personal information, which FNBZ will only process where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour (**special personal information**).

FNBZ processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with FNBZ's obligations under certain pieces of legislation.

FNBZ will not retain or process special personal information unless one of the statutory exceptions applies. For example, (where a statutory exception is to obtain consent) specific consent for the processing of biometric personal information may be requested by FNBZ.

Special personal information is personal information about the following:

- your religious beliefs.
- your philosophical beliefs (for example where you enter a competition and you are requested to express your philosophical view).
- your race (like where you apply for a product or service where the statistical information must be recorded)
- your ethnic origin.
- your trade union membership.
- your political beliefs.
- your health (like where you apply for an insurance policy).
- your sex life (like where you apply for an insurance policy).
- your biometric information (like to verify your identity); and / or

your criminal behaviour and alleged commission of an offence (like to prevent money laundering as required by law or when you apply for employment or enter into a relationship with us.

3.4 Purposes for the processing of personal information

Personal information will be processed by FNBZ in the normal course of business of managing employees for various purposes:

- For required banking information in order to process an employee's remuneration.
- To suggest the opening of a bank account on behalf of the employee in order to secure staff rates.
- To admit the employee to the relevant pension, retirement, or provident funds and/or medical aid providers.
- To comply with the group's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented by the group. This will include

conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the employee, or prospective employee, including but not limited to Register of Employees' Dishonesty System (REDS), Politically Exposed Person (PEP), relevant fraud prevention agencies and services and reference checks where FirstRand is not allowed to allow employees to act in certain roles and capacities if they are guilty of fraud or dishonesty. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment.

- To comply with all applicable laws authorising or requiring such processing, including (but not limited to): all employment and labour related laws, laws relating to the safety of employees as work and laws relating to financial crime, fraud, money laundering, KYC, sanctions, combatting of crime and corruption and other corporate laws and their regulations.
- To carry out the specific obligations and duties of FNBZ in the field of employment legislation.
- To realise objectives laid down by, or by virtue of tax or other applicable legislation.
- To properly assess performance under an employment contract.
- To undertake management activities, such as succession planning, talent management, training, work planning, task management, assessment of employee performance, and to control security and access to facilities.
- To market products, goods and services to the employee, the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels, research or statistical purposes and/or the creation of employee-specific product offerings; and/or otherwise securing and facilitating the employee's employment with the group, including rendering to the employee value added services (such as employee wellbeing initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees.
- To share spouse/children personal information for business purposes, e.g., for business travel purposes, events, etc.
- To share children's details, e.g. beneficiary of pension on the death of a parent.
- To share close relatives' details – next of kin/emergency contact persons.
- To compile statistics and results from research studies and related programs.
- To process in order to send work-related communications to the employee's mobile device via the FNB app.

The purposes above are mandatory for employees to provide their personal information to enable the processing of:

- the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract, or
- compliance with legal obligations to which FNBZ is subject

- the protection of a legitimate interest of the employee
- the legitimate interests pursued by FNBZ, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

- for a prospective employee: to FNBZ being unable to enter into an employment contract with that prospective employee
- for an employee: to disciplinary sanctions, where applicable or, in extreme cases, such refusal may lead to dismissal.

There may be instances where FNBZ will lawfully process personal information for purposes not listed above.

Where the provision of personal information is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

When Will We Process Your Personal Information?

We will only process your personal information for lawful purposes relating to our business if the following applies:

- if you have consented thereto.
- if a person legally authorised by you, the law or a court, has consented thereto.
- if it is necessary to conclude or perform under a contract, we have with you.
- if the law requires or permits it.
- if it is required to protect or pursue your, our or a third party's legitimate interest; and / or

3.5 Quality of personal information

FNBZ will take reasonable and practicable steps to ensure that the personal information of employees is complete, accurate and not misleading, and is updated where necessary.

The group's human capital functions have provided the self-service channels, through which employees are required to update personal information if it changes. The onus is on the employee to utilise this channel to update his/her personal information, when necessary.

For updates to personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

3.6 Security and confidentiality of personal information

All personal information processed by FNBZ will be held confidentially.

FNBZ will take reasonable, appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation. Our security measures (including physical, technological and

procedural safeguards) will be appropriate and reasonable. This includes the following:

- keeping our systems secure (like monitoring access and usage)
- storing our records securely.
- controlling the access to our buildings, systems and/or records; and
- safely destroying or deleting records.

3.7 Retention of personal information

Personal information will not be kept by FNBZ for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNBZ reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and FNBZ.

Other than in the aforementioned instances, FNBZ may request the employee's consent for the further retention of personal information and will state the reasons for making such a request.

3.8 The transfer of personal information

Employees' personal information may be shared within the FirstRand Group and with third parties with whom FNBZ contracts to process such personal information and pursuant to the instruction of FNBZ, under specific terms or terms as set forth in this notice for the purposes mentioned above.

Provided that FNBZ ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of FNBZ and in accordance with this notice, FNBZ may transfer personal information within the group, operators (see 3.9 below) or other third parties based outside Zambia if FNBZ` has a lawful justification and such transfer complies with the law, e.g. a signed a contract requiring the other party to adhere to such standards of security and fair handling in respect of the information as are adhered to by FNBZ,.

3.9 Use of operators

An operator is a person who processes personal information on behalf of FNBZ in terms of a contract or mandate, without coming under the direct authority of FNBZ.

FNBZ may assign the processing of FNBZ employee personal information to an operator which will process the personal information only with the knowledge or authorisation of FNBZ.

FNBZ will contract with the operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by FNBZ.

3.10 Employees' privacy rights

3.10.1 Access to information

An employee has the right to access the personal information which relates to him/her. Certain personal information relevant to the employee may be accessed through the self-service channel.

3.10.2 Right to correction of personal information

The employee has the right to correct inaccurate personal information which relates to him/her. The employee is able to update and correct certain types of personal information stored on the human capital

platform using the self-service channel (Oracle). For instructions on how to do so, the employee should contact the responsible person in their Human Capital Department.

For updating other types of personal information, the employee should address a simple request to that effect to the responsible human capital department. Should FNBZ be unable to correct the personal information, FNBZ, must explain its position in writing to the employee.

Should FNBZ refuse the correction, the employee is entitled to request that a statement be attached to the personal information, which indicates that a correction has been sought and not made.

3.10.3 Right to de-identification/destruction/deletion

The employee is entitled to require the de-identification/destruction/deletion of his/her/their personal information, which is by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- legally prohibited from being recorded, communicated or retained; or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a simple request to that effect to the responsible human capital department.

FNBZ must delete/remove/destroy this personal information or explain in writing its position regarding the request. Should FNBZ refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the personal information, which indicates that a request for removal of personal information has been sought and not made.

3.10.4 Right to complain

Employees have the right to submit a complaint to the information regulator in their country (if such office, or a similar office, had been created) regarding an alleged breach of the conditions for lawful processing of personal information.

An employee can choose to submit complaints to FNBZ for resolution before submission to the information regulator. Any queries or complaints regarding the employee's personal information can be directed to the respective human capital manager within FNBZ.

3.11 Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice and for access to information about his or her personal information processed within the context of this notice, (e.g., employee discloses his health status to his line manager, who then communicates this to the entire office) the employee may contact their Data Privacy Officer or their Human Capital Department.

FNBZ must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

3.12 Reference to other FNB Zambia policies

- FNBZ acceptable use of information resources policy:

The FNBZ's acceptable use of information resources policy aims to ensure effective, efficient and secure use of FNBZ information resources and informs employees of what is deemed acceptable and unacceptable practice. Subject to the terms of this notice, FNBZ will monitor the use of its information resources by employees. This notice also contains requirements and guidelines for dealing with the personal information of clients.

- FNBZ Internal Privacy Policy.
- FNBZ Privacy Framework.

Where there is a conflict between Local Laws and FirstRand Policies, the local laws shall prevail to the extent of the inconsistency.

-END-

FNB Eswatini Employee Privacy Notice

Document Control	
Notice Owner:	Executive Head – Human Capital
Version:	1
Approved by: EXCO	Date Approved:
Reviewable	Every 3 years / subject to changes in law

FNB Eswatini Employee Privacy Notice

TABLE OF CONTENTS

FNB Eswatini Employee Privacy Notice

1. Objective & Purpose

1.1. The protection of the privacy of personal information of employees is very important to FNB. To protect the privacy of personal information, FNB follows general principles in accordance with the Data Protection Act No. 5 of 2022.

1.2. The employee Privacy Notice has been developed to help employees understand how FNB collects, uses, and safeguards their personal information

1.3. The Notice includes general information regarding the Bank's treatment of employees' Personal Information and employees' rights and responsibilities in respect of their Personal Information.

2. Scope

This Notice applies to all employees, defined for purposes throughout this document as current, past and prospective employee that is, permanent, and temporary employees, as well as fixed term contractors or independent contractors contracted by FNB.

3. Definition of Employees' Personal Information

3.1. For the purpose of this Notice, and other documents referred to in this Notice, personal information means information about an identifiable, living, natural person.

3.2. By way of examples, an employee's personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

3.3. Personal Information does not include aggregated or anonymised information where such information is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only.

3.4. Personal Information includes the following types of information:

3.4.1 Personal details, but is not limited to, e.g. name, address, location information, online identifier, emergency contact details, birth certificate, employee number or identity number, educational and other qualifications; curriculum vitae.

3.4.2 Job-related details: e.g. start date, place of work, salary, benefits, absence records.

3.4.3 Financial information: e.g. bank account number.

3.4.4 Performance/evaluation information: e.g. whether an employee performs job duties in accordance with the relevant requirements.

3.5. An employee undertakes to communicate his/her Personal Information to FBN and First Rand when specifically requested by FNB to do so.

4. Sensitive Personal Information

4.1. Sensitive personal information to include genetic data, data related to children, data related to offences, criminal sentences or security measure, and biometric data, as well as, if it is processed for what it reveals, personal information revealing racial or ethnic origin, political opinions, or affiliations, religious or philosophical beliefs, affiliation, trade-union membership, gender, and data concerning health or sex life.

4.2. There are special categories of an employee's Personal Information which FNB will only process where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour (Sensitive Personal Information).

4.3. FNB processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with FNB's obligations under the Occupational Health and Safety Act, 2001.

4.4. FNB will not retain or process Sensitive Personal Information unless one of the statutory exceptions applies. For example, (where a statutory exception is to obtain consent) specific consent for the processing of biometric personal information may be requested by FNB.

5. Basis for the Processing of Personal Information

5.1. The legal bases for the processing of personal data are:

5.1.1 the data subject provides explicit consent to the processing.

5.1.2 it is necessary for the conclusion or performance of a contract to which the data subject is a party.

5.1.3 it is necessary for compliance with a legal obligation to which the data controller is subject.

5.1.4 it is necessary to protect the legitimate interests of the data subject.

5.1.5 it is necessary for the proper performance of public law duty by a public body; or

5.1.6 it is necessary for pursuing the legitimate interests of the data controller or a third party to whom the information is supplied.

6. Purposes for the Processing of Personal Information

6.1. Personal Information will be processed by FNB in the normal course of business of managing employees for various purposes:

6.1.1 Requires banking information in order to process an employee's remuneration.

6.1.2 To suggest the opening of a bank account on behalf of the employee, in order to secure staff rates.

6.1.3 Admitting the Employee to the FNB Retirement Benefit Structure and/or Retirement Fund, Provident Fund and/or medical aid providers.

6.1.4 Complying with FNB and the Group's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented by the Group. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the Employee or prospective Employee, including but not limited to Register of Employees' Dishonesty System (REDS), Politically Exposed Person (PEP), Anti-Corruption Commission (ACC), the Financial Intelligence Unit (FIU), and the Eswatini Central Bank for reference checks. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment.

6.1.5 Complying with all applicable laws authorising or requiring such processing, including (but not limited to):; the Employment Act, 1980; the Industrial Relations Act, 2000; and the Occupational Health and Safety Act 85 of 2001; the Money Laundering and Financing of Terrorism Financing (Prevention) Act, 2011 with its Amendement (2016); The Suppression of Terrorism Act, 2008 and the Companies Act, 2009.

6.1.6 Conducting criminal, credit, reference, and other related reference checks on the employee or prospective employee, including Register of Employees' Dishonesty System (REDS), Financial Intelligence Unit (FIU), and the Eswatini Central Bank reference checks.

6.1.7 Carrying out the specific obligations and duties of FNB in the field of employment legislation.

6.1.8 Realising objectives laid down by or by virtue of tax or other applicable legislation.

6.1.9 Properly assessing performance under an employment contract.

6.1.10 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.

6.1.11 Marketing of products, goods and services to the Employee, the Employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels, research or statistical purposes and/or the creation of Employee specific product offerings; and/or otherwise securing and facilitating the Employee's employment with the Group, including rendering to the employee value added services (such as employee wellness initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees.

6.1.12 Sharing spouse/ children Personal Information for business purposes. E.g. for business travelling purposes, events etc.

6.1.13 Sharing of children details for e.g. beneficiary of pension, on the death of a parent.

6.1.14 Sharing of close relative's details – next of kin/emergency contact persons.

6.1.15 Compile statistics and results from research studies and related programs.

6.1.16 Processing in order to send work related communications to the employee's mobile device via any of FNB's platforms including the First Rand and WesBank apps.

6.2 The purposes above are mandatory for employees to provide their Personal Information to enable the processing of:

6.2.1 the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract,

6.2.1 compliance with legal obligations to which FNB is subject, or

6.2.2 the protection of a legitimate interest of the employee; or

6.2.3 the legitimate interests pursued by FNB, or by the third party to whom the Personal Information is disclosed for the above purposes.

6.3 If an employee refuses to provide the required Personal Information for these purposes, this may lead:

6.3.1 for a prospective employee: to FNB being unable to enter into an employment contract with that prospective employee, and

6.3.2 for an employee: to disciplinary sanctions, where applicable, or in extreme cases such refusal may lead to dismissal.

6.3.3 There may be instances where FNB will lawfully process Personal Information for purposes not listed above.

6.3.4 Where the provision of Personal Information is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

7. Quality of Personal Information

7.1 FNB will take reasonable and practicable steps to ensure that the Personal Information of employees is complete, accurate and not misleading, and is updated where necessary.

7.2 FNB HR has provided the self-service channels, through which employees are required to update Personal Information if it changes. The onus is on the employee to utilise this channel to update his/her Personal Information, when necessary.

7.3 For updates to the Personal Information that are not made possible through the Self-Service channel, employees are required to address the relevant request to the responsible HR Department.

8. Security and Confidentiality of Personal Information

8.1. All Personal Information processed by FNB will be held confidentially.

8.2. FNB will take reasonable, appropriate technical and organisational measures to keep Personal Information secure in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

8.3. HC has an obligation to notify the Commission and affected data subjects when a data breach or security compromise occurs. This obligation falls on both FNB or any other third party processing personal information under the authority of a FNB.

9. Retention of Personal Information

9.1. Personal Information will not be kept by FNB for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNBreasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and FNB.

9.2. Other than in the aforementioned instances, FNB may request the employee's consent for the further retention of Personal Information and will state the reasons for making such a request.

10. The Transfer of Personal Information

Employees' Personal Information may be shared within the FirstRand Group and with third parties with whom FNB and FirstRand contracts to process such Personal Information and pursuant to the instruction of FNB and First Rand.

11. Use of Data Processor

11.1. A data processor is a natural person, or public body which processes personal information for and on behalf of a data controller and under the instructions of a data controller and excludes persons who are authorised to process data under the direct authority of a controller.

11.2. FNB may assign the processing of FNB employee Personal Information to a data processor which will process the Personal Information only with the knowledge or authorisation of FNB.

11.3. FNB will contract with the data processor to ensure that Personal Information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by FNB.

12. Employees' Privacy Rights

12.1 Access to Information

12.1.1 The employee has the right to access the Personal Information which relates to him or her. Where an employee wishes to request Personal Information, which they do not have a direct right to, but which information is needed to protect a right of the employees a request must be addressed to HC.

12.1.2 Where HC denies an employee a request for access to information, the data subject shall be entitled to be given written reasons for the denial.

12.1.3 An employee has a right to challenge the written reasons for denial or requests made.

12.2 Right to Correction of Personal Information

12.2.1 The employee has the right to correct inaccurate Personal Information which relates to him or her. The employee is able to update, and correct certain types of Personal Information stored on the Human Capital Platform using the Self-Service channel. For instructions on how to do so, the employee should contact the responsible person in the HR Department.

12.2.2 For updating other types of Personal Information, the employee should address a simple request to that effect to the responsible HR Department. Should FNB be unable to correct the Personal Information, FNB d must explain its position in writing to the employee.

12.2.3 Should FNB refuse the correction, the employee is entitled to request that a statement be attached to the Personal Information which indicates that a correction has been sought and not made.

12.3 Right to de-identification/destruction/deletion

12.3.1 The employee is entitled to require the de-identification/destruction/deletion of his/her/their Personal Information which is, by reference to the objectives of the processing:

12.3.1.1 inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

12.3.1.2 legally prohibited from being recorded, communicated or retained, or retained beyond a reasonable period after the end of the employment contract between the parties.

12.3. 2 To do so, the employee should address a simple request to that effect to the responsible HR Department.

12.3.3 FNB must delete/remove/destroy this Personal Information or explain in writing its position regarding the request. Should FNB refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the Personal Information which indicates that a request for removal of Personal Information has been sought and not made.

12.4 Right to object to direct marketing

An employee is entitled to object to the processing of their personal data by FNB for direct marketing purposes.

12.5 Right to complain

12.5.1 Employees have the right to submit a complaint to the Eswatini Communications Commission ('the Commission') regarding an alleged breach of the conditions for lawful processing of personal information as set out in DPA.

12.5.2 Employees have the right to submit a complaint to HC.

13 Contact Persons

13.1 For any Personal Information protection issues, questions or complaints concerning the application of the Notice and for access to information about his or her Personal Information processed within the context of this Notice, (e.g. Employee discloses his HIV status to his line manager, who then communicates this to the entire office) the employee may contact FNB Data Privacy Officer, line Manager or Human Capital Business Partner (HCBP).

13.2 FNB must record in writing any employee or third-party complaint relating to the disclosure of employee Personal Information, and respond to that complaint, keeping a record of such response.

14 Reference to other FNB Policies

14.1 FNB Eswatini Data Quality Management Policy

14.2 FNBE Data Privacy and Protection ('Privacy') Framework

14.3 FNB Eswatini Internal Privacy Policy

14.4 FNBE Direct Marketing Consent Policy

14.5 FNBE Privacy Incident Management Minimum Standard

14.6 FNBE Cookie Notice

14.7 FNBE Privacy Implementation Standard (With Annexures A,C,D,E,F)

These Policies are available on the intranet at:

https://international/fnbSwaziland/dataprivacy/Forms/AllItems.aspx

RMB Nigeria Employee Data Privacy Notice

TABLE OF CONTENTS

1. BACKGROUND AND PURPOSE

Protecting the privacy of personal information of its employees is very important to Rand Merchant Bank Nigeria Limited (hereinafter referred to as "**RMB NIGERIA**"). To do so, RMB NIGERIA follow general principles in accordance with applicable privacy laws and, particularly, the Nigeria Data Protection Act, 2023 and the Nigeria Data Protection Regulation 2019.

RMB NIGERIA has developed the following employee privacy notice (**notice**) to help employees understand how RMB NIGERIA collects, use and safeguard its personal information.

This notice includes general information regarding RMB NIGERIA's treatment of employees' personal information and employees' rights and responsibilities in respect of their personal information.

2. SCOPE

This notice applies to all employees, defined for purposes throughout this document as current, past and prospective employees (that is, permanent and temporary employees), as well as fixed-term contractors or independent contractors contracted by RMB NIGERIA.

3. DISCLOSURE INFORMATION RELATED TO EMPLOYEES' RIGHTS AND RESPONSIBILITIES IN RESPECT OF THEIR PERSONAL INFORMATION.

RMB NIGERIA will process personal information collected from its employees.

Definition of Employees' Personal Information

For the purpose of this notice, and other documents referred to in this notice, personal information means information about an identifiable, living, natural person.

By way of example, an employee's personal information may include an employee's race, gender, identification number, employee number, residential address, telephone number, date of birth, marital status, disability, biometric information, and correspondence sent or received by an employee that is implicitly or explicitly private or confidential.

Personal information does not include aggregated or anonymised information where RMB NIGERIA is incapable of identifying an employee. Aggregated or anonymised information includes any information about an employee, which may be included as part of a statement about a group of employees or a graph or pie chart showing characteristics as part of a group of employees only. For instance, *"20% of RMB NIGERIA's employees own or use a laptop computer"* is not personal information.

Personal information, processed by RMB NIGERIA, regarding its employees (**personal information**) includes the following types of information:

- personal details, including but not limited to, name, address, location information, online identifier, emergency contact details, birth certificate number, employee number or identity number, educational and other qualifications, and curriculum vitae.
- job-related details, e.g. start date, place of work, salary, benefits, absence records; financial information, e.g. bank account number;
- performance/evaluation information, e.g. whether an employee performs their job duties in accordance with the relevant requirements.

An employee of RMB NIGERIA hereby consents to communicate his/her personal information to RMB NIGERIA when specifically requested by RMB NIGERIA to do so.

Definition of Employees' Sensitive Personal Data

There are special categories of an employee's personal information, which RMB NIGERIA will only process where a heightened set of requirements are met. These special categories are information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and certain information relating to criminal offences and criminal behaviour (**sensitive personal data**).

RMB NIGERIA processes medical and health related information with the employee's consent for the purposes of insurance and medical aid agreements concluded on the employee's behalf and for his/her benefit, and in order to comply with RMB NIGERIA's obligations under relevant legislation.

RMB NIGERIA will not retain or process sensitive personal data unless:

(a) am employee has given and not withdrawn consent to the processing for the specific purpose or purposes for which it will be processed.

(b) processing is necessary for the purposes of performing the obligations of the RMB Nigeria or exercising rights of the employee under employment or social security laws or any other similar laws.

(c) processing is necessary to protect the vital interests of the employee or of another person, where the employee is physically or legally incapable of giving consent.

Purposes For the Processing of Personal Information

Personal information will be processed by RMB NIGERIA in the normal course of business of managing employees for various purposes:

1. For required banking information in order to process an employee's remuneration.
2. To suggest the opening of a bank account on behalf of the employee, in order to secure staff rates.
3. To admit the employee to the relevant pension, retirement, or provident funds and/or medical aid providers.
4. To comply with the Group's anti-money laundering, terrorist financing, fraud and corruption detection obligations as well as risk management processes implemented by the Group. This will include conducting criminal, credit, reference, sanctions, anti-bribery and other related reference checks on the employee, or prospective employee, including but not limited to Register of Employees' Dishonesty System (REDS), politically exposed person (PEP), relevant fraud prevention agencies and services and reference checks where RMB NIGERIA is not allowed to allow employees to act in certain roles and capacities if they are guilty of fraud or dishonesty. Such checks may be conducted on an ongoing basis throughout the period of employment and may include lifestyle audits as well as reporting on the conduct of employees where required to do so by law to the relevant bodies after termination of employment.
5. To comply with all applicable laws authorising or requiring such processing, including (but not limited to): all employment and labour related laws, laws relating to the safety of employees as work and laws relating to financial crime, fraud, money laundering, KYC, sanctions, combatting of crime and corruption and other corporate laws and their regulations.
6. To carry out the specific obligations and duties of RMB NIGERIA and the Group in the field of employment legislation.
7. To realise objectives laid down by, or by virtue of, tax or other applicable legislation.
8. To properly assess performance under an employment contract.
9. To undertake management activities, such as succession planning, talent management, training, work planning, task management, assessment of employee performance, and to control security and access to facilities.

10. To market products, goods and services to the employee, the employee's involvement in pilots relating to new or updated products, services, platforms, goods and channels, research or statistical purposes and/or the creation of employee-specific product offerings; and/or otherwise securing and facilitating the employee's employment with the Group, including rendering to the employee value added services (such as employee wellbeing initiatives and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of employees.
11. To share spouse/children personal information for business purposes, e.g. for business travel purposes, events, etc.
12. To share children details, e.g. beneficiary of pension on the death of a parent.
13. To share close relatives' details – next of kin/emergency contact persons.
14. To compile statistics and results from research studies and related programs.
15. To process in order to send work-related communications to the employee's mobile device via any of the group's platforms including the RMBN, RMB, FNB and WesBank apps.

The purposes above are mandatory for employees to provide their personal information to enable the processing of:

1. the performance of the employment contract to which the employee is party or in order to take steps at the request of the prospective employee prior to entering into the employment contract, or
2. compliance with legal obligations to which RMB NIGERIA is subject, or
3. the protection of a legitimate interest of the employee; or
4. the legitimate interests pursued by RMB NIGERIA, or by the third party to whom the personal information is disclosed for the above purposes.

If an employee refuses to provide the required personal information for these purposes, this may lead:

1. for a prospective employee: to RMB NIGERIA being unable to enter into an employment contract with that prospective employee, and
2. for an employee: to disciplinary sanctions, where applicable or, in extreme cases, such refusal may lead to dismissal.

There may be instances where RMB NIGERIA will lawfully process personal information for purposes not listed above. Where the provision of personal information is not for a lawful process, a separate, written consent from the employee (which consent may at any moment be withdrawn) will be sought.

Quality of Personal Information

RMB NIGERIA will take reasonable and practicable steps to ensure that the personal information of each employee is complete, accurate and not misleading, and is updated where necessary.

The Group's human capital functions have provided the self-service channels, through which employees are required to update personal information if it changes. The onus is on the employee to utilise this channel to update his/her personal information, when necessary.

For updates to personal information that are not possible through the self-service channel, employees are required to address the relevant request to the responsible human capital department.

Security and Confidentiality of Personal Information

All personal information processed by RMB NIGERIA will be held confidentially. RMB NIGERIA will take reasonable, appropriate technical and organisational measures to keep personal information secure, in accordance with its policies and procedures on information security, and in accordance with any applicable legislation.

Retention of Personal Information

Personal information will not be kept by RMB NIGERIA for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where RMB NIGERIA reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by a contract between the employee and RMBN.

Other than in the aforementioned instances, RMB NIGERIA may request the employee's consent for the further retention of personal information and will state the reasons for making such a request.

Transfer of Personal Information

Employees' personal information may be shared within the Group and with third parties with whom RMB NIGERIA contracts to process such personal information and pursuant to the instruction of RMB Nigeria, under specific terms or terms as set forth in this notice for the purposes mentioned above. In accepting the employment offer of RMB NIGERIA, the employee of RMB NIGERIA hereby consents to such transfer of personal information. A simplified legal entity structure for the Group can be found at https://www.firstrand.co.za/the-group/ownership-and-legal-structure/.

Provided that RMB NIGERIA ensures adequate safeguards and/or enters into a contract for third parties to process personal information for the purposes mentioned above, pursuant to the instruction of RMB NIGERIA and in accordance with this notice, RMB NIGERIA may transfer personal information within the Group, to Operators (as defined in "Use of Operators" below) or other third parties based in or outside Nigeria if RMB NIGERIA has a lawful justification, e.g. a signed contract requiring the other party to adhere to such standards of security and fair handling in respect of the information as are adhered to by RMBN, regardless of whether the laws of the countries in which such third parties reside provide sufficient safeguards regarding the processing of personal information.

Use of Operators

An Operator is a person who processes personal information on behalf of RMB NIGERIA in terms of a contract or mandate, without coming under the direct authority of RMBN.

RMB NIGERIA may assign the processing of RMB NIGERIA employee personal information to an Operator, and such Operator must process the personal information only with the knowledge or authorisation of RMBN.

RMB NIGERIA will contract with the Operator to ensure that personal information is kept confidential, and subject to such standards of security and fair handling in respect of the information as are adhered to by RMB NIGERIA.

Employees' Privacy Rights

Access to Information

The employee has the right to access the personal information which relates to him/her. Certain personal information relevant to the employee may be accessed through the self-service channel.

Right to Correction of Personal Information

The employee has the right to correct inaccurate personal information which relates to him/her. The employee is able to update, and correct certain types of personal information stored on the human capital platform using the self-service channel. For instructions on how to do so, the employee should contact the responsible person in his/her human capital department.

For updating other types of personal information, the employee should address a simple request to that effect to the responsible human capital department. Should RMB NIGERIA be unable to correct the personal information, RMB NIGERIA must explain its position in writing to the employee.

Should RMB NIGERIA refuse the correction, the employee is entitled to request that a statement be attached to the personal information, which indicates that a correction has been sought and not made.

Right to De-Identification/Destruction/Deletion

The employee is entitled to require the de-identification/destruction/deletion of his/her/their personal information, which is by reference to the objectives of the processing:

- inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
- legally prohibited from being recorded, communicated or retained; or
- retained beyond a reasonable period after the end of the employment contract between the parties.

To do so, the employee should address a simple request to that effect to the responsible human capital department.

RMB NIGERIA must delete/remove/destroy such personal information or explain in writing its position regarding the request. Should RMB NIGERIA refuse the employee's request for de-identification/destruction/deletion, the employee is entitled to request that a statement be attached to the personal information, which indicates that a request for removal of personal information has been sought and not made.

Right to Complain

Employees have the right to submit a complaint to the Nigeria Data Protection Commission (if such office, or a similar office, had been created) regarding an alleged breach of the conditions for lawful processing of personal

information where employee has made a compliant to the Head of Human Capital and the DPO of RMB NIGERIA and a response is not provided within 14 working days.

An employee must therefore submit complaints to RMB NIGERIA for resolution before submission to the Commission. Any queries or complaints regarding the employee's personal information can be directed to the Head of Human Capital and the DPO of RMB NIGERIA.

Contact persons

For any personal information protection issues, questions or complaints concerning the application of the notice and for access to information about his or her personal information processed within the context of this notice, (e.g. employee discloses his HIV status to his line manager, who then communicates this to the entire office) the employee may contact Head of Human Capital and the DPO of RMB NIGERIA.

RMB NIGERIA must record in writing any employee or third-party complaint relating to the disclosure of employee personal information, and respond to that complaint, keeping a record of such response.

-END-

Data privacy notice for employees, workers and contractors

Version Control

Version	Author	Date	Comments
1	L Hayward	December 2022	Policy launched
2	J Robinson	April 2024	Annual review

Policy Owner	Accountable Executive	Approval Tier
Lizzie Hayward, Head of Employee Relations	Duncan McIntyre – People Director	Tier 3

Effective Date	Date of Next Review
April 2024	April 2025

Introduction

Aldermore Group PLC and its subsidiaries (including Aldermore Bank PLC and MotoNovo Finance Limited) (**"we", "us", "our"** or **"Aldermore"**) provide this Data Privacy Notice to inform our employees, workers and contractors of our policy relating to the processing of their personal information.

This Data Privacy Notice sets out the basis on which we will process your personal information. Please read the notice carefully to understand our practices regarding your personal data and how we will use it.

This notice should be read in conjunction with our Data Protection Policy in force from time to time.

This Data Privacy Notice does not form part of any contract of employment or contract to work or provide services and may be amended at any time.

You will see that we mention the privacy policies of other organisations we share information with (including Cifas). We do need to share these with you and copies are available on the intranet . Please read them carefully and contact those organisations if you have questions (their details are in their policies).

About Us

Aldermore is the data controller of the personal data of its employees, workers and contractors and is subject to applicable data protection laws.

Aldermore

Contacting us:

If you have any questions about this Data Privacy Notice or your information or wish to exercise any of your rights as described in this Data Privacy Notice or under applicable data protection laws, you can contact our Data Protection Officer:

Email: DPO@aldermore.co.uk

Address:

Data Protection Officer

Aldermore

4th Floor

40 Spring Gardens

Manchester

M2 1EN

What types of data are protected

Personal data

This Data Privacy Notice applies to your "personal data", that is any information relating to you as an identified or identifiable person.

Special categories of personal data

Within the broad range of information which can be personal data, the following are "special categories of personal data" which are subject to a greater degree of protection:

- physical or mental health
- racial or ethnic origin
- political opinions
- trade union membership
- religious or similar beliefs
- sexual life or sexual orientation
- genetic and biometric data

What information we collect

Information you give us

You may give us information about you by filling in forms or by corresponding with us by phone, email, in person, or otherwise. This includes information you provide when you first applied for employment or engagement with us.

To assist us in complying with our obligation to maintain accurate information you should immediately notify Aldermore in writing of any changes to your personal details. Such changes may include but are not limited to:

- your name, change of address or telephone number or mobile telephone number;
- nationality or immigration status, date of marriage, or civil partnership, marital status or civil partnership status or divorce;
- change of life assurance beneficiary;
- change of address, telephone number etc. of next of kin or emergency contact;
- bank details;
- arrest, prosecution or conviction for a criminal offence;
- any disciplinary action taken against you by a professional or regulatory body; or
- if you become bankrupt, apply for or have made against you a receiving order, make any composition with your creditors or commit any act of bankruptcy.

Failure to comply with this requirement may constitute a disciplinary offence.

Where you have notified us or we otherwise become aware of an inaccuracy in your information we will take steps to ensure that information is erased or rectified without delay.

Information we collect about you

- We collect personal information to operate our business and manage your work, monitor performance and to comply with our legal obligations as an employer and/or a contracting party.
- We may collect, store and use information about your use of our IT system and about your computer, tablet, mobile or other device through which you access our IT system.
- We may also collect information from other sources, such as those which are commercially available to us.
- The information about you that we may collect includes, but is not limited to, the following:
    - name;
    - home address;
    - contact details (such as telephone number and email address);
    - date of birth;

- gender;
- marital status;
- copies of your passport, driving licence and similar documents;
- data we obtain from fraud prevention agencies (see Cifas below)
- education history, training, qualifications, professional experience;
- current and past employment details;
- immigration status and work permits;
- languages spoken and level of proficiency;
- other information given in your CV;
- performance records and appraisals;
- information related to equal opportunities monitoring;
- sickness absence and sickness management (including information about your health, including any medical condition and health records);
- emergency contact details (which may also include personal data of next of kin, family or friends);
- absence records (including holiday, sickness absence and family-related leave);
- appraisals and relevant disciplinary and grievance records;
- information about your remuneration and benefits and payroll information, including National Insurance number; and
- images recorded on CCTV which operates in the building and at all internal and external entrances to the building.

We also collect data derived from our IT and communications systems, including:

- recording building access through the security access system and CCTV installed in the building and at all entrances (both external and internal);
- monitoring website browsing, use of the instant messaging service and employee or contractor access to electronic files and systems.
- monitoring e-mail usage;
- your location;
- chat records, and audio and video recordings of meetings; and
- videos or photos that we make public for marketing purposes (for example if we film you in the office or in the related workplace).

Special categories of personal data

Your information includes such “special categories of personal data” (see the description provided above) as you and any medical professionals provide to us.

Information provided by third parties

Some of the information we collect (as described above), and additional information, may be provided to us by recruitment agencies with whom you have registered an interest. Such recruitment agencies support our recruitment processes under a duty of confidentiality.

During the recruitment process we may also research information regarding your skills, experience or qualifications and comments and opinions made public on social networking sites such as LinkedIn, Facebook, Instagram and Twitter.

We may also receive other information about you from organisations such as HMRC, credit reference agencies, fraud prevention agencies (including Cifas), sanction screening, criminal convictions screening (including disclosure and barring service) and referees.

Data relating to criminal convictions & offences

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions in the following ways:

- to assess your suitability for a role; and
- to carry out statutory checks.

We will use your personal information in this way to comply with our legal, regulatory and corporate governance obligations and for our legitimate interests to prevent and detect criminal activity to ensure good employment practices. We have in place an appropriate policy and safeguards which we are required by law to maintain when process such data.

Data relating to the internal fraud database (Cifas)

We will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct carried out by their staff and potential staff. “Staff” means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term.

Further details of how your information will be used by Cifas, and your data protection rights, can be found by visiting the Cifas website where a copy of the full notice is available at www.cifas.org.uk/fpn. A copy of this is available on the intranet.

What we do with your information and on what basis

We process your information (other than special categories of personal data) for the reasons listed below. The legal justification for the processing of the information is in each case one or more of the following (specific examples are given for each).

Processing is necessary for the performance of your contract

We have obligations towards you under the terms of your contract (for example, we are contractually obliged to pay you any money due under your contract). Equally, you have contractual obligations to us, both as part of entering into contract and in the ongoing performance of it. In order for us to ensure that both we and our employees, workers and contractors can perform our contractual obligations, we may process your information for the following purposes:

- recruitment processes (including negotiation and communicating with you in relation to your application);
- considering your suitability for employment or work, taking up your reference; and conducting appropriate checks;
- induction processes;
- workforce planning (including consideration for promotion and other roles and decisions about promotions and workforce restructurings);
- management of absence (including absence due to illness or injury);
- complying with our legal obligations and for other purposes;
- training and training records;
- payroll processes and administration (including the deduction of trade union fees and conferring benefits and any applicable termination payments such as statutory redundancy pay);
- monitoring performance;
- disciplinary and grievance investigations, hearings and decisions;
- criminal records checks;
- to carry out identity checks, your right to work in the UK, anti-money laundering checks and checks with Fraud Prevention Agencies pre-application, at the application stage and periodically after that. Where you have been introduced to us by an agency or other intermediary they may do these searches on our behalf;
- corporate reporting and regulatory good practice disclosures in respect of Aldermore's workforce, workforce remuneration, workforce policies and related issues;
- undertaking business analysis activities;

- to process information about a crime or offence and proceedings related to that;
- administration of your day to day duties relating to your employment; and
- managing tax, pensions and healthcare insurance payments.

Where we have a legal or regulatory obligation

UK and EU law and certain regulations require us to process employee or contractor information in order to comply with our legal obligations. In order for us to do so, we may process your information for the following purposes:

- preventing illegal working;
- complying with health and safety obligations;
- liaising with HMRC and other government entities or agencies in relation to attachments of earnings and similar deductions;
- assessing fitness and propriety of individuals for regulatory purposes and communicating with the Prudential Regulation Authority, the Financial Conduct Authority and other relevant public or regulatory bodies;
- providing regulatory references;
- to ensure the safety and security of our systems;
- dealing with requests by you to exercise your rights under data protection laws;
- to conduct regular screening checks to identify links to any politically exposed persons, special interest persons, adverse media, or any financial sanctions, and to comply with our anti-money laundering obligations; and
- carrying out equal opportunities monitoring.

Where we have a legitimate interest

Data protection law allows us to process employee, worker or contractor information where it is necessary for the purposes of our legitimate interests. We consider it to be in our legitimate interests to process your information for the following purposes:

- dealing with any legal disputes involving you or other current or prospective or former employees, workers or contractors;
- ensuring or evidencing that Aldermore's or any employee's, worker's or contractor's confidential information has not been misused or disclosed;
- ensuring safety and security of those working for us;
- analysing retention and attrition rates;
- to administer our IT system including troubleshooting, data analysis, testing, research, statistical and survey purposes;

- to improve our IT system to ensure that content is presented in the most effective manner for you and for your computer, mobile device or other item of hardware through which you access our IT system;

- as part of our efforts to keep our IT system safe and secure and to monitor compliance with our related policies;

- making decisions about promotions, career progression, work allocation and termination of any contract of employment or contract to work or provide services;

- to administer your pension scheme, family-related pay, and any insured benefits and to perform ancillary functions;

- to provide a reference; and

- to contact former or existing employees or contractors for work related or reference related reasons.

We may also monitor employee or contractor performance and behaviour through the information we collect about you during the course of your employment or engagement on the basis of our legitimate interests. This includes by:

- recording employee or contractor telephone lines (if applicable);

- recording building access through CCTV installed in the building and at all entrances (both external and internal);

- blocking emails from being sent to clients when there is a concern regarding information being sent;

- monitoring access to websites from employee IP addresses and employee access to electronic files and systems for the purpose of identifying unusual patterns that might indicate a cyber-attack or fraudulent behaviour is occurring.

If you do not agree with the processing of your information on the basis that it is in Aldermore's legitimate interests to do so, please inform us using the contact details at the beginning of this Data Privacy Notice, following which we shall cease to process your information for that purpose, unless certain exceptions apply: see "Right to object to processing in certain circumstances" under "Your rights" below.

Special categories of personal data

Where we process "special categories of personal data" we will ensure we are permitted to do so under data protection laws. We may process such data for the purposes of:

- carrying out the obligations we have to exercise both Aldermore's and your specific rights which are imposed or conferred by employment laws including, where it is in the public interest, monitoring equality opportunities, assessing suitability for particular jobs and to consider whether adjustments may need to be made to accommodate an employee or contractor with a disability;

- establishing, defending and bringing legal claims; and

- in the case of information about your physical or mental health (including information contained in sickness records) to enable Aldermore to monitor sick leave, assess your working capacity, administer benefits, take decisions as to an employee's or contractor's working capacity and for occupational health purposes.

Disclosure of your information to third parties

For the purposes set out above, we may share your information with:

- our group companies;
- third-party suppliers;
- professional advisors (including lawyers, accountants and auditors);
- your previous employers to verify your employment history;
- academic institutions to verify your qualifications;
- Cifas, who will use it to verify your identity and prevent fraud, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct. Further details of how your information will be used by us and Cifas, and your data protection rights, can be found by visiting the Cifas website where a copy of the full notice is available at www.cifas.org.uk/fpn;
- external companies who make reference requests (dates of employment and last position held only will be confirmed) unless further information is requested, for instance under the Senior Management and Certification Regime (SMCR) roles;
- prospective sellers or buyers in the event Aldermore buys or sells any business or assets;
- our insurers;
- providers of employee screening services ; and
- law enforcement agencies and governmental and regulatory bodies such as HM Revenue & Customs, Financial Conduct Authority, the Prudential Regulation Authority, the Ombudsman, the Information Commissioner's Office and under the Financial Services Compensation Scheme.

We may also share your information with other parties which provide products or services to Aldermore, such as any payroll administrator, benefits provider and IT services providers, in order to enable us to achieve the purposes set out above. Our third party service providers and business partners are subject to security and confidentiality obligations and are only permitted to process your personal information for specified purposes and in accordance with our instructions.

Third party benefit providers with whom we share your information are:

- our pensions provider;

- our payroll administrator;
- our private medical insurance provider;
- our Group Income Protection provider;

You have been notified of the identity of the relevant benefit provider and any changes or additions will be communicated to you by email or other appropriate method.

Save as set out in this Data Privacy Notice, or as required by law, we do not sell your personal information or disclose it to any third parties without your consent.

Information about data subjects connected to you

In connection with the administration of your pension scheme and/or family-related pay and any insured benefits that (as applicable) Aldermore may collect your family members' (such as a parent, grandparent, great-grandparent, child or sibling) personal data. This will be limited to the name, address, phone number and email address of the relevant family number. We may also collect family members' personal data for administrative purposes in connection with the operation of your contract using "next of kin" forms. Processing of such data for the purposes set out in this section is necessary for our legitimate interest. As it is not reasonable for us to communicate with such family members directly, please let us know if any such family member objects to us processing their data in accordance this section (including sharing of such data with the relevant insurers). In the case of children under the age of 13, any applicable consent or objection, or other relevant communication should come from someone with parental responsibility for them. You must ensure that you notify Aldermore of any changes to such information without undue delay.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration;
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights; and
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We use automated processing at the application stage to assess your right to work in the UK. This means we attempt to match your personal details to publicly available information through sources such as the Royal Mail or Cifas. If for any reason we are unable to complete our

formalities using this process you will be informed how you many complete the process using manual methods.

Policies and procedures

We implement a number of additional policies in relation to data privacy and data security, including but not limited to those listed below.

- Aldermore Cookie Policy
- Aldermore Information Security Policy
- Applicant Privacy Policy
- Background Checking Policy
- Criminal Offence Data Policy
- Data Protection Policy
- Information Retention Schedule
- Information Security Policy

Please familiarise yourselves with these additional policies. If you have any questions about such policies and procedures you should speak to your line manager without delay or to our Data Protection Officer.

Any new or updated policies or manual will be communicated to you by email, via Aldermore's intranet or any other appropriate method.

Please read them carefully and contact those organisations if you have questions (their details are in their policies).

Security of your information

We are committed to ensuring that your information is safe and take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Data Privacy Notice.

All information you provide to us electronically is stored on our secure servers within the United Kingdom, Germany and South Africa. Please see 'International Transfers' below for further information.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of our IT system, you are responsible for keeping this password confidential. We ask you not to share your passwords with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your information, we cannot guarantee the security of your data transmitted to or stored on our IT system and any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

Aldermore

How long we keep your information

We will keep your data on our live systems for the applicable periods as set out in the Information Retention Schedule, , or for as long as we are required by law or in order to comply with a regulatory obligation during and following the end of your employment or engagement. However, beyond such applicable periods, your data will be archived in accordance with our business continuity and backup procedures, which is available on the intranet. Where personal data is archived and held for business continuity and backup purposes, it will not be accessible on Aldermore's live systems and will not be used for any other purposes.

Your rights

Access to your information and updating your information

- You have the right to access information which we hold about you. If you so request, we shall provide you with a copy of your personal information which we are processing and hold about you ("data subject access request"). For any further copies which you may request, we may charge a reasonable fee based on administrative costs.

- You also have the right to receive your personal information in a structured and commonly used format so that it can be transferred to another data controller ("data portability").

- We want to make sure that your personal information is accurate and up to date. You may ask us to correct or remove information you think is inaccurate.

Right to object to processing in certain circumstances

You also have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal information which is based on our legitimate interests. Where you object on this ground, we shall no longer process your personal information unless:

- the processing is nevertheless necessary for the performance of your contract; or

- the processing is necessary for the establishment, exercise or defence of legal claims; or

- we have a legal or regulatory obligation for which the processing of the information is necessary; or

- we can demonstrate that our legitimate interest is sufficiently compelling to override your fundamental rights and freedoms.

Your other rights

- You also have the right to request that we rectify your information if it is inaccurate or incomplete.

- In certain limited circumstances, you have the right to: request the erasure of your personal information ('right to be forgotten').

- You also have the right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.

Exercising your rights

You can exercise any of your rights as described in this Data Privacy Notice and under data protection laws by contacting us via the details given in the "Contacting us" box above.

Save as described in this Data Privacy Notice or provided under data protection laws, there is no charge for the exercise of your legal rights. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the data or taking the action requested; or (b) refuse to act on the request.

Where we have reasonable doubts concerning the identity of the person making the request, we may request additional information necessary to confirm your identity.

International transfers

As an international organisation, we may transfer your information to any country in which we operate. Therefore, it may be necessary to transfer your details to members of our group or third-party service providers located in countries that may not offer equivalent data protection or privacy laws to those in the UK. We may:

- transfer your data to our group entities based in South Africa; and
- store your data in servers based in Germany.

Under data protection laws, we can only transfer your personal data to a country outside the UK where:

- the UK government has decided the particular country ensures an adequate level of protection of personal data (known as an '**adequacy regulation**') further to Article 45 of the UK GDPR;
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for you; or
- a specific exception applies under relevant data protection law.

Where we transfer your personal data outside the UK, we do so on the basis of an adequacy regulation or (where this is not available) or an appropriate safeguard .

Details regarding these safeguards can be obtained from our Data Protection Officer whose details are given above. Complaints

You also have the right to complain to the Information Commissioner's Office ("**ICO**") (https://ico.org.uk/) about our data processing activities. The ICO also has a dedicated helpline at 0303 123 1113. We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Changes

This Data Privacy Notice may be amended by Aldermore at any time it is sole and absolute discretion. Any changes which may be made to this Data Privacy Notice in the future will be notified to you by email and on our intranet.

Governance
The policy is governed in accordance with the Policy Approval structure of the Group Policy Framework and is deemed to be a Tier Three Policy:

Tier	Definition
One	Matters Reserved for the Board and approval of key Group policies, including any material amendments thereto from time to time. Tier One policies also include those which require approval at Board Risk Committee and/or Board Audit Committee (highest materiality).
Two	Committee or Accountable Executive responsibility.
Three	**Accountable Executive or delegate**

Consent for the processing of Personal Data

The law on data protection is contained within the Data Protection (Jersey) Law 2018 which requires that an employer must have a lawful reason for collecting and using personal data and ensure that this is processed fairly, for a limited period of time, and kept accurate and secure.

The purpose of this Consent is to inform you of how, as a Data Controller, Ashburton (Jersey) Limited ("Ashburton" "we" "our"), manages Personal Data under current and forthcoming legislation and regulations. Please read this statement so that you know and understand the purposes for which we collect, use and may disclose your Personal Data.

In order to comply with our obligations under legislation regarding Employment, Financial Services and Anti-Money Laundering, we have a duty to keep records about our employees, including those persons employed on a temporary or contractual basis. We therefore collect, record, store, adapt, process and transfer certain personal information about you as part of our general employee records.

Our records may include your address and contact details, marital status, educational background, employment application and history, history with Ashburton, areas of expertise, details of salary and benefits, bank details, tax and social security numbers, performance appraisals and salary reviews, records relating to holiday and other leave, training and development information, and other management records. We have obtained this information in a number of ways, either directly from you, from other third parties and otherwise over time through our relationship with you and may receive and/or retain it in various forms (whether in writing, electronically, verbally or otherwise).

We use this information for the purposes of human resources administration and employee, work and general business management purposes. For example, we need this information to administer payroll (including the payment of ITIS and employee social security contributions); improve and maintain the administration of employee benefits (such as leave entitlement); facilitate the management of work and employees; operating performance and salary reviews, and in order for us to comply with record keeping and other legal obligations.

We process information relating to your health, which may amount to special category data being held. The particular information that we hold relating to your health is the records of sickness absence and medical certifications. The purpose of keeping this sort of information is to administer company and statutory sick pay, monitor and manage sickness absence and comply with obligations under the law, (e.g. Social Security sickness benefits). We may also process specific information regarding any medical conditions or allergies of which you have informed us to ensure that in an emergency the correct information may be given to an attending medical practitioner.

We will keep your data for a period of 10 years after you leave the employment of Ashburton.

Your personal information will also be sent to our corporate parent in South Africa, to provide them with management information in respect of divisional employees, financial budgeting and so that they can carry out the administration of employee records and benefits. The FirstRand Group, which includes Ashburton Investments, is in a jurisdiction outside the European Economic Area ("EEA") but has security measures in place which will ensure the confidentiality of the information. Some of your data may also be sent to contractual benefit providers so that they may manage or administer your salary, pension and healthcare (medical) insurance, if appropriate to your employment status. We may also appoint third party business partners to provide various training programmes to employees, in which case some of your personal information will be provided to them.

We may take photographs or video film of you for Group internal use or publicity purposes. These images may be published in our printed publications, on our website or other social media sites such as Facebook or Twitter, or in any publicity material about our products and services sent to the news media. These images may be seen worldwide and not just where Jersey or EU laws apply.

You have a right to access the personal data that we hold about you and may ask for rectification in cases where such data is inaccurate or incomplete. You also have the right to request that we delete data about you where there is no compelling reason for its continued processing. Further details about your rights under data protection legislation can be obtained from Jersey's Office of the Information Commissioner.

You are reminded of Ashburton's Employee People Practices Manual which states that all telephone calls are recorded.

By signing this form, you acknowledge and consent to Ashburton processing personal data relating to you for the purposes explained above, and specifically, you give your consent with regard to the processing of:

i. special category data relating to any health matter; and
ii. the transfer of your personal data to FirstRand Group members outside the EEA; and
iii. the use of my photographic image

If you have any questions, please contact the Human Resources Department.

Signature: _____

Name _____ Date: _____

VOLKSWAGEN FINANCIAL SERVICES

FINANCE. LEASE. INSURANCE. MOBILITY.

VOLKSWAGEN FINANCIAL SERVICES SOUTH AFRICA (PTY) LTD. • PO BOX 784162 • SANDTON, 2146

POLICY APPROVAL POSITIONING PAPER

VWFS POPIA Employee Privacy Policy

1 Purpose of the policy

The purpose of the Volkswagen Financial Services South Africa's Employee Privacy Policy is to outline the commitment of its employees, as good corporate citizens, to comply with the provisions of privacy legislation and regulation and to ensure that personal information in the possession of VWFS SA, as well as personal information collected by VWFS SA is protected and secured against any unlawful collection, retention, dissemination, and use.

2 Impact of the policy

- Board of Directors
- Senior Management
- Regulatory Risk Management function
- VWFS SA Employees

3 Key changes to the previous policy

This policy has been previously approved by the VWFS SA Board and tabled at the MRC. The policy is therefore being reviewed as per policy governance requirement (on a bi ennial basis (every 2 years)) and is being re-tabled for review, with no material changes having been made.

4 I-OHB reference

Developed to added POPIA Regulation Compliance.

5 Recommendation

This policy is submitted to Management Risk Committee and then to the VWFS SA Board for noting.

VOLKSWAGEN FINANCIAL SERVICES

FINANCE. LEASE. INSURANCE. MOBILITY.

VOLKSWAGEN FINANCIAL SERVICES SOUTH AFRICA (PTY) LTD. • PO BOX 784162 • SANDTON, 2146

Protection of Personal Information Act (POPIA)

Employee Privacy Policy

Level	Group
Framework owner	Information Office
Approving Committee	VWFS Management Risk
Date	07 June 2022
Noting Committee	Board Risk Committee
Date	21 June 2022

Table of Contents

1. DEFINITIONS

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

Child	A natural person under the age of 18 years old who is not legally competent, without the assistance of a competent person, (i.e. a parent or guardian) to take any legal or what type of action or decision in respect of any matter concerning him or herself.
Competent person	Any person who is legally competent to consent to any legal or what type of action or decision being taken in respect of any matter concerning a child (i.e. a parent or guardian).
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data subject	Means the person to whom Personal Information relates to. In reference to VWFS SA this means, primarily but without limitation, customers, employees, operators or suppliers, and third parties.
Employee	Means a person employed for wages or salary, including permanent employees, non-permanent employees, contractors, secondees and contingent workers.
Information Officer and Deputy Information Officer	Means the person responsible to ensure overall compliance to privacy legislation as prescribed by the POPI Act.
Information Regulator	Means any independent national authority responsible for upholding the fundamental right of individuals to data privacy through the enforcement and monitoring of compliance with data protection legislation in that jurisdiction under the POPI Act and PAIA Act.
Juristic Person	Means an existing company, trust, non-profit organisation, association 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 personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. This means any party that provides a service to process information on behalf of VWFS SA.

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 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
POPIA	Protection of Personal Information Act 4 of 2013
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 merging, linking, as well as restriction, degradation, erasure or destruction of information.
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 (c) regardless of when it came into existence.
Responsible Party	Means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
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 any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

2. BACKGROUND AND PURPOSE

Confidentiality of information and the secure retention thereof are entrenched concepts in the financial services industry. How information is handled and protected has become increasingly important and Privacy Legislation dictates that VWFS SA become compliant to all the requirements. It is important to understand the significance and value of information as a business asset which enables, better product offering, research and marketing positioning.

The purpose of the Volkswagen Financial Services South Africa's **("VWFS SA")** Employee Privacy Policy ("**Policy**") is to outline the commitment of VWFS SA employees, as good corporate citizens, to comply with the provisions of privacy legislation and regulation and to ensure that personal information in the possession of VWFS SA, as well as personal information collected by VWFS SA is protected and secured against any unlawful collection, retention, dissemination and use.

This policy governs the handling of personal information by VWFS SA and its employees and establishes a set of principles for the collection, retention, processing, dissemination and general good management of personal information in the possession of VWFS SA as well as the responsibilities of all employees of VWFS

SA. The policy will set the parameters to consequences that will follow in the event of a data breach occurring as a result of mismanagement of information in any manner.

With jurisdictions outside of South Africa, laws and regulations which are of a higher standard than this policy will take precedence over this policy. However, where this policy is of a higher standard it will take precedence. In addition, if an international operation is required to comply with privacy related legislation that is considered more onerous than stated in this policy it will take precedence.

Furthermore, this policy aims to protect the privacy rights of persons, both natural and juristic, in instances where VWFS SA and/or any operator that may process personal information on behalf of VWFS SA, is processing personal information. In such instances, VWFS SA is deemed to be the responsible party. Privacy legislation, specifically the Protection of Personal Information Act as well as the Promotion of Information Act endeavours to balance, on the one hand, the fundamental right of the data subject to privacy and, on the other hand, the legitimate need for private and public bodies to obtain and process personal information for various business-related purposes. This balance is achieved through universally accepted privacy principles or conditions which will be incorporated and explained in this policy. This policy includes general information regarding VWFS SA's treatment of employees, customer and supplier's personal information and employees, customers and suppliers' rights and responsibilities in respect of their personal information.

3. APPLICABILITY AND SCOPE

All VWFS SA employees are responsible for acquainting themselves with this policy and ensuring that they know, understand and comply with the provisions thereof. Failure to comply could result in significant risk to VWFS SA and its business operations where PI, SPI and children's PI are processed. This policy applies to all VWFS SA business units that process PI, SPI and children's PI internally within the business and to all operators that process such information on behalf of VWFS SA.

This policy applies to any device or process and business procedure within VWFS SA's information processing facilities and all PI, SPI or children's PI, either new or existing, in electronic, paper-based form, or on any other form. This policy must be read in conjunction with applicable and relevant VWFS SA policies and guidance notes as communicated periodically.

4. PRINCIPLES APPLICABLE TO THE HANDLING OF PI AND SPI

All VWFS SA employees 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, internal policies, as well as applicable privacy and any other laws. In the event that a provision of this policy conflicts with any other provisions or policy not governing PI, then the provisions of this policy will take precedence. The applicable privacy principles are as follows:

Privacy Principle 1: Accountability

All VWFS SA employees will ensure that all processes and procedures that handle and deal with PI, SPI and children's PI from its collection, processing, dissemination, retention and destruction complies with applicable local and international privacy legislation and regulation. In pursuance of compliance with these, the following will be established:

- A privacy governance structure and formal privacy reporting;
- Formal privacy policies and supporting standards and procedures;
- A privacy framework (including appropriate privacy roles, responsibilities, and accountabilities).

VWFS SA will remain the responsible party for all PI, SPI and children's PI processed under its control and authority and will ensure that adequate contracts with operators are concluded where PI, SPI and children's PI is processed by a third-party provider or operator.

An Information Officer and / or a Deputy Information Officer will be appointed and be held responsible for addressing all privacy-related queries, including queries relating to this policy. A group-wide privacy awareness programme will be established and provided to all employees at induction and/or on an ongoing basis.

Privacy Principle 2: Processing Limitation

VWFS SA and its employees will process PI, SPI and children's 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. Collection of all PI, SPI and children's PI will be directly received from the data subject (or from the parent or legal guardian, in the case of a child's PI or an authorised intermediary). This means that PI, SPI and children's PI will be collected throughout the relationship with VWFS SA through various interactions including, but not limited to, collection required by law. A data subject's PI, SPI and children's PI may be collected from a third party as long as the conditions in law are adhered to.

Minimality

VWFS SA will only process PI, SPI and children's PI that is relevant, adequate and not excessive in relation to the purpose for which the information was intended for.

Justification

To achieve transparency, a valid justification for the processing of PI, SPI and children's PI will be disclosed by VWFS SA to data subjects, either before the collection of the PI, SPI and children's PI or as soon as reasonably practical thereafter.

Consent to process PI, SPI and Children's PI

VWFS SA and its employees will ensure that PI, SPI and children's PI is processed with the necessary consent, or where a lawful justification or legitimate interest exists, for example where VWFS SA has a legitimate business requirement to process PI. As such, VWFS SA must comply with the following rules relating to consent:

- All consent obtained is to be voluntary, specific and informed consent.

- Prior to the processing of PI, SPI or children's PI, VWFS SA must ensure that consent has been obtained from the data subject, especially where it is necessary to conclude a contract with the data subject or to provide a service. In all other cases VWFS SA will ensure that the required consent is obtained as soon as reasonably practicable. VWFS SA must ensure that such consent is stored and can be retrieved in the event of a dispute involving a data subject. PI, SPI and children's PI will only be processed in a manner that is necessary to comply with contractual obligations or according to the justifiable grounds as required by legislations.
- Consent need not be obtained if:
    - Processing is an obligation imposed by law on VWFS SA and its entities or subsidiaries;
    - processing protects a legitimate interest of the data subject;
    - processing is necessary to protect the legitimate interests of VWFS SA and its entities or subsidiaries or a third party with whom the PI, SPI and children's PI are shared;
    - Processing is needed to conclude or perform in terms of a contract with the data subject.
- VWFS SA 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.
- VWFS SA 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 and this policy).
- Where the processing of PI, SPI or children's PI is based upon the legitimate interest of the data subject, responsible party or a third party with whom the PI is shared, the exception must be that VWFS SA will only process SPI with the specific consent of the data subject and will adhere to the limitations that apply to the processing of SPI (as outlined in this policy).

Consent Mechanisms for processing customer, employee and supplier PI and SPI by VWFS SA

The consent, where necessary and declaration should be incorporated in the contractual documentation presented to the data subject for the relevant products, services or goods. Additionally, VWFS SA must make the Customer Privacy Policy available to the data subject in an appropriate manner upon request.

The terms relating to the consent for data subjects who are employees of VWFS SA can be found in the POPIA consent declaration. All new and existing permanent and non-permanent employees of VWFS SA must sign this declaration, thereby acknowledging the consent provided by these data subjects (see Annexure A).

Usage of the PI, SPI and Children's PI collected by VWFS SA

PI will be collected for a specific, explicitly defined and lawful purpose related to a function or business activity of VWFS SA. All data subjects, whose PI is processed, will be made aware of the purpose of the processing of their PI, per principle 6 of this policy.

Objection to the processing of PI and SPI by a data subject

In the event that a data subject (or parent or competent person in relation to a child) objects to the processing of their PI, SPI and children's PI, VWFS SA will stop processing that PI within a reasonable

time unless there is an obligation for VWFS SA 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.

Privacy Principle 3: Purpose Specification

VWFS SA 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 VWFS SA. This will be disclosed to the data subject when the PI, SPI and children's PI is collected from the data subject or by a third party or will be disclosed as soon thereafter as reasonably possible.

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

PI, SPI and children's PI belonging to employees of VWFS SA will be processed for the purposes of providing remuneration to the employees; conducting criminal, credit, reference, and other related reference checks on the employee or prospective employee, including The Association for Savings & Investment SA (ASISA) and Financial Advisory and Intermediary Service Act (FAIS) reference checks; carrying out the specific obligations and duties of VWFS SA 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 and/or pension schemes.

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

VWFS SA will not retain records of PI, SPI and children's PI for 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. VWFS will use POPIA as guidance with regard to the retention of records.

VWFS SA may retain records of PI, SPI or children's PI beyond its stipulated retention period only for historical, statistical, regulatory reporting or research purposes. Such retention will be done in line with the applicable privacy and security safeguards of VWFS SA and in line with the legislative requirements of POPIA.

Privacy Principle 4: Further Processing

Further processing of a data subject's PI, SPI and children's PI will only be permitted if this processing is compatible with the original purpose of collection and processing, as specified in the Customer Privacy Policy and the Supplier contract.

Further processing of PI, SPI and children's PI will be allowed for the following reasons:

- if obtained from a public record,

- if further processing is required by law,
- to protect a public interest or matters of national security, or
- by authorisation of the applicable Information Regulator;
- if the customer has specifically consented thereto;
- if a person legally authorised by the customer, the law or a court, has consented thereto;
- if it is necessary to conclude or perform under a contract the organisation has with the customer;
- if it is required to protect or pursue the customers, the organisations or a third party's legitimate interest; and / or
- if the customer is a child and a competent person (like a parent or guardian) has consented thereto.

Privacy Principle 5: Information Quality

VWFS SA and its employees 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. VWFS SA must also ensure that channels are available for employees to update their PI, SPI and children's PI in the event that it changes.

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

Privacy Principle 6: Openness

VWFS SA will allow access to information in terms of the provisions of PAIA. VWFS SA must ensure that the PAIA Manual is updated to cater for the provisions of POPIA.

VWFS SA 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. VWFS SA will make available to the data subject:

- the name and address of the business 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 as provided for in the PAIA Manual.

Privacy Principle 7: Security Safeguards

VWFS SA 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, SPI and children's 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.

VWFS SA must ensure that all permanent and non-permanent employees are trained on measures to prevent loss, damage and unauthorised access or destruction of PI, SPI and children's PI under its control.

Taking into account that PI, SPI and children's PI is processed on behalf of VWFS SA by third-party service providers or operators, these service providers or 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 the contractual agreements.

VWFS SA will, as part of its 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. VWFS SA 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.

VWFS SA 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. Such incidents must be reported to the Information Officer. The Information Officer must conduct an investigation to determine if such an incident must be reported to the Information Regulator and affected data subjects in terms of privacy legislation. VWFS SA 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 included in the directory.

Privacy Principle 8: Data Subject Participation

VWFS SA and its employees will ensure that it has processes in place whereby data subjects can enquire as to what information VWFS SA holds on them, as set out in the VWFS SA PAIA Manual. 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.

VWFS SA must implement the required channels that enable data subjects to approach VWFS SA as prescribed in the PAIA manual, in order for VWFS SA to confirm whether it holds PI, SPI and children's PI about the data subject, free of charge. Moreover, VWFS SA will be required to provide the record or a description of the PI, SPI and children's PI held by VWFS SA, or an operator, within a reasonable period of time; in the prescribed format and may levy the prescribed charges provided for in terms of the PAIA manual. Where VWFS SA provided a record or description of the PI, SPI and children's PI, VWFS SA will advise the data subject that they may request a correction or deletion of the information. Such correction or deletion of the PI, SPI and children's PI will be entertained by VWFS SA if the PI, SPI and children's PI is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, and in line with the applicable legislative requirements. The Information Officer will have the final say in this regard.
Subject to privacy regulations, VWFS SA will ensure that it prescribes a complaints resolution process which will outline the manner for receiving and investigating privacy related complaints; and co-operating with the Information Regulator on such complaints.

Privacy Principle 9: Cross-Border Transfer of Personal Information

PI, SPI and children's PI in the possession of VWFS SA may be transferred to a third-party in another country if:

- the PI, SPI and children's PI will be adequately protected under the other country's laws or an agreement with the third-party recipient;
- 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;
- the data subject has consented to the transfer; and / or
- it is not reasonably practical to obtain the data subject's consent, but the transfer is in the data subject's interest.

All cross-border transfers of PI, SPI and children's PI will be subject to the terms of this policy and applicable legislation and legal requirements in that jurisdiction.

Privacy Principle 10: Third-Party / Operator Management

VWFS SA will ensure that third party suppliers or operators processing any PI, SPI and children's PI on its behalf have adequate technical and organisational measures to prevent loss, damage and unauthorised access to or destruction of VWFS SA PI, SPI and children's PI under the control of the third-party service provider or operator by means of conclusion of a contract. Regular monitoring of third-party suppliers or operators will be undertaken by VWFS SA, to ensure that the PI, SPI and children's PI handled by the third-party supplier or operator is dealt with legally and in accordance with the Supplier Privacy Policy as well as applicable SLA's as and when required.

The Supplier Privacy Policy as well as applicable SLA's must include contractual provisions relating to confidentiality of PI, SPI and children's PI; processing limitations; legal requirements, incident reporting and termination provisions for third-party suppliers or operators.

5. GENERAL

Non-compliance with this policy and all related policies, standards, procedures and directives may result in disciplinary action or dismissal of any transgressing employee. In addition, the regulatory penalties for non-compliance include:

- Administrative fines of up to R 10 million or as per jurisdiction, whichever is the greater and depending on the category of the data breach incident; or
- Imprisonment of up to ten (10) years; or
- Deportation; and
- Penalties from more than one jurisdiction may also apply.

6. OWNERSHIP AND REVIEW

This policy is owned by the VWFS SA Information Office and must be reviewed at least every two (2) years. This policy will also be reviewed when any applicable code of conduct under POPIA is published or there is any amendment to the overarching legislation.

7. Policy Administration

Title	VWFS SA Employee Privacy Policy
Author	Nirusha Maharaj
Owner	VWFS Information Office
Document version	Version 2.0
Version date	31 May 2022

Revision summary

Framework Name	Version	Approval Date
VWFS SA Employee Privacy Policy	V1.0	12 August 2019
VWFS SA Employee Privacy Policy	V2.0	07 June 2022

Review

Frequency of review	Next review date	Last review date
Biennially or as required	2024	2019

8. Annexure A:

POPIA Consent and Disclosure for Employees

The Protection of Personal Information Act, 2013 ("**POPIA**").

1. The Employee consents to:

1.1 the processing of the Employee's personal information (PI), special personal information (SPI) and children's personal information (PI) (as defined by POPIA), any affiliate company and/or any third parties including agents/contractors authorised by the organisation to process the PI, SPI and children's PI; and

1.2 the transfer of the Employee's PI, SPI and children's PI to any member of the VWFS Group outside of the Republic of South Africa; for the purposes of:

1.2.1 remunerating the Employee;

1.2.2 admitting the Employee to the Pension Fund and/or Provident Fund and/or medical aid providers;

1.2.3 conducting criminal, credit, reference, and other related reference checks on the Employee, including but not limited to), South African Fraud Prevention Services (Shamwari), Life Offices' Association (LOA) and Financial Advisory and Intermediary Service Act (FAIS) reference checks;

1.2.4 complying with laws authorising or requiring such processing, including (but not limited to): the Basic Conditions of Employment Act 75 of 1997; the Labour Relations Act 66 of 1995; the Employment Equity Act 55 of 1998; and the Occupational Health and Safety Act 85 of 1993; and/or

1.2.5 otherwise securing and facilitating the Employee's employment with Volkswagen Financial Services (Pty) Ltd ("VWFS SA"), including rendering to the employee Value Added Services (such as employee wellness and catering services), employee administration, training, performance reviews, talent management and other reasons related to the management of staff.

2. The Employee consents to the VWFS SA accessing its records held by VWFS SA or at any other institution if VWFS SA has a reasonable suspicion that the Employee has committed a criminal act, including but not limited to fraud and money laundering.

3. The PI, SPI and children's PI will be stored by VWFS SA:

3.1 for no longer than is necessary to achieve the purpose for which it was collected, unless further retention is:

3.1.1. required by law, regulatory reporting or contractual obligation;

3.1.2. otherwise reasonably required by VWFS SA for lawful purposes related to its functions and activities; or

3.1.3. retained further with the Employee's consent;

3.2. after which point the PI, SPI and children's PI will be de-identified;

3.2.1 in hard copy and/or electronic copy; and

3.2.2. subject to security safeguards that are adequate to ensure the integrity and confidentiality of the PI, SPI and children's PI.

4. The Employee acknowledges that the PI, SPI and children's PI supplied to VWFS SA is accurate and correct and undertakes to update VWFS SA of any changes in the PI, SPI and children's PI as soon as reasonably practicable to do so.

5. The Employee has the right:
5.1. of access to and the right to rectify the Personal Information collected; and
5.2. to object at any time, on reasonable grounds relating to the employee's particular situation, in which event the consequences of the objection will be explained to the Employee, unless legislation provides for such processing.

6. The Employee may be subjected to disciplinary procedures in terms of VWFS SA's Disciplinary Policy should s/he fail to comply with POPIA.

7. The Employee warrants that
7.1. any PI, SPI and children's PI provided by the Employee in relation to the Employee's spouse is provided with the permission of the Employee's spouse; and
7.2. any PI, SPI and children's PI provided by the Employee in relation to a child is provided in the Employee's capacity as the legal guardian of that child or with the authorisation from the child's legal guardian.
7.3. The Employee acknowledges that the PI, SPI and children's PI provided in relation to the Employee's spouse and a child will be used by VWFS SA for the purpose of providing the Employee's spouse and that child with any benefits to which such spouse or child is entitled

8. Personal Information includes, but is not limited to:
8.1. personal details: e.g. name, address, location information, online identifier, emergency contact details, birth certificate number, employee number, identity number, educational and other qualifications; curriculum vitae;
8.2. job-related details: e.g. start date, place of work, salary, benefits, absence records;
8.3. financial information: e.g. bank account number;
8.4. performance/evaluation information: e.g. whether you performed your job duties in accordance with the relevant requirements, and whether you exceeded those requirements, whether you met your job goals.

9. Special Personal Information includes, but is not limited to:
9.1. medical and health-related information;
9.2. information about race;
9.3. criminal information

10. Children's Personal Information includes, but is not limited to:
10.1. information regarding children under the age of 18 years old.