



FirstRand

FIRSTRAND GROUP CUSTOMER PRIVACY NOTICE

July 2024

## TABLE OF CONTENTS

|    |   |    |
|----|---|----|
| 1  | INTRODUCTION .....  | 3  |
| 2  | SCOPE.....  | 3  |
| 3  | DEFINITIONS.....  | 3  |
| 4  | BACKGROUND AND PURPOSE OF THIS NOTICE .....   | 4  |
| 5  | RESPONSIBLE PARTIES .....   | 5  |
| 6  | CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL INFORMATION BY THE BANKING<br>INDUSTRY .....   | 5  |
| 7  | WHAT IS PERSONAL INFORMATION? .....   | 6  |
| 8  | WHEN WILL THE GROUP PROCESS CUSTOMERS' PERSONAL INFORMATION?.....   | 7  |
| 9  | WHEN WILL THE GROUP PROCESS CUSTOMERS' SPECIAL PERSONAL INFORMATION? .....  | 7  |
| 10 | WHEN AND HOW WILL THE GROUP PROCESS THE PERSONAL INFORMATION OF CHILDREN?...  | 7  |
| 11 | WHEN AND FROM WHERE DOES THE GROUP OBTAIN PERSONAL INFORMATION ABOUT<br>CUSTOMERS?.....   | 8  |
| 12 | REASONS THE GROUP NEEDS TO PROCESS CUSTOMERS' PERSONAL INFORMATION .....  | 10 |
| 13 | WHY DOES THE GROUP FURTHER USE OR PROCESS CUSTOMERS' PERSONAL INFORMATION?<br>.....   | 14 |
| 14 | CENTRALISED PROCESSING.....   | 15 |
| 15 | ENRICHING PERSONAL INFORMATION .....  | 15 |
| 16 | HOW DOES THE GROUP USE CUSTOMERS' PERSONAL INFORMATION FOR REWARDS? .....   | 16 |
| 17 | HOW DOES THE GROUP USE PERSONAL INFORMATION FOR DIRECT MARKETING?.....  | 17 |
| 18 | WHEN WILL THE GROUP USE CUSTOMERS' PERSONAL INFORMATION TO MAKE AUTOMATED<br>DECISIONS ABOUT THEM? .....  | 18 |
| 19 | WHEN, HOW AND WITH WHOM DOES THE GROUP SHARE CUSTOMERS' PERSONAL<br>INFORMATION? .....  | 19 |
| 20 | WHEN AND HOW DOES THE GROUP OBTAIN CUSTOMERS' PERSONAL INFORMATION FROM<br>CREDIT BUREAUX AND WHEN WILL IT SHARE CUSTOMERS' PERSONAL INFORMATION WITH<br>CREDIT BUREAUX?..... | 20 |
| 21 | UNDER WHICH CIRCUMSTANCES WILL THE GROUP TRANSFER CUSTOMERS' PERSONAL<br>INFORMATION TO OTHER COUNTRIES?.....   | 21 |
| 22 | CUSTOMERS' DUTIES AND RIGHTS REGARDING THE PERSONAL INFORMATION THE GROUP<br>HOLDS ABOUT THEM.....  | 22 |
| 23 | HOW THE GROUP SECURES CUSTOMERS' PERSONAL INFORMATION .....   | 25 |
| 24 | HOW LONG DOES THE GROUP KEEP CUSTOMERS' PERSONAL INFORMATION?.....  | 25 |
| 25 | HOW THE GROUP PROCESSES PERSONAL INFORMATION ABOUT PERSONS RELATED TO A<br>JURISTIC PERSON .....  | 25 |

26 CESSION, DELEGATION OR ASSIGNMENT .....26  
27 CHANGES TO THIS NOTICE .....26  
28 ANNEXURES .....27  
29 SCHEDULE OF LEGISLATION..... 28

## 1 INTRODUCTION

FirstRand Limited (FirstRand or the group) follows a multi-branding approach. The logos of some of the group's major brands are shown below.



A representation of FirstRand's simplified legal entity structure can be found on the group's website at <https://www.firstrand.co.za/the-group/ownership-and-legal-structure/>.

## 2 SCOPE

This notice applies to the FirstRand group of companies as defined in the definitions section. The various companies in the group offer financial and non-financial solutions. These solutions include transactional, lending, investment, insurance, telecommunication and consumer products, goods and services. In this notice, solution means any financial and non-financial product, service or goods offered by a group company.

## 3 DEFINITIONS

### WHAT IS "FIRSTRAND" OR "THE GROUP"?

In this notice, references to "FirstRand" or "the group" are to FirstRand Limited and its subsidiary companies, including divisions, segments and business units. Certain subsidiary companies may be excluded from the group description (such as where the group is involved in private equity investments). Confirmation as to whether this notice applies to a specific company (a registered legal entity) associated with the group can be sought through the contact details provided in this notice. In this notice, any reference to "the group" or "FirstRand" 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.

### WHAT IS THE "PLATFORM"?

In this notice, references to the group's platform mean the platform provided by a company within the group which is a collection of service channels, solutions and interfaces (like apps and websites), including that of the group's agents and independent third-party service providers.

### WHO IS A CUSTOMER?

For this notice, the definition of a "customer" includes:

- prospective customers (persons who are interested in the group solutions or to whom the group may be offering or promoting products or services solutions);
- new and existing customers (persons who have taken up group solutions);
- previous customers (persons who previously took up group solutions); and
- users (persons who use group platforms, interfaces or service channels).

#### **WHAT IS “PROCESS”?**

In this notice “process” means how the group collects, uses, stores, makes available, destroys, updates, discloses or otherwise deals with customers’ personal information.

The examples provided in this notice are for illustrative purposes and are not exhaustive.

#### **4 BACKGROUND AND PURPOSE OF THIS NOTICE**

**Protecting customers’ personal information is important to FirstRand and it follows general principles under applicable privacy laws.**

This notice helps the group’s customers understand how the group collects, uses and safeguards their personal information. This notice also outlines customers’ privacy rights and how the law protects them.

The group collects personal information about its customers. This includes what customers tell the group about themselves, what the group learns from a customer or when a customer makes use of a solution or interacts with the group’s platform through various interfaces and service channels.

This notice may also apply to other parties (such as authorised agents and contractors) acting on the group’s behalf when providing customers with solutions, interfaces or service channels. If a FirstRand group business processes personal information for another party under a contract or a mandate, the other party’s privacy policy or notice will apply.

The group may combine customers’ personal information (across the group’s platform, interfaces, service channels or companies) and use the combined personal information for any of the purposes stated in this notice.

If a customer uses the group’s platform, group solutions or service channels and interfaces, or accepts any rules, agreements, contracts, mandates or annexures with the group, or uses any solutions offered by the group, the customer agrees to the processing by the group of the customer’s personal information as stated in this notice. Please note that the group may not be able to continue a relationship with a customer, provide a customer with certain solutions or permit access to the group’s platform (including service channels and interfaces) if the customer does not agree to the notice.

#### **IMPORTANT:**

Where it is necessary to obtain consent for processing, the group will seek a customer’s consent separately. Customers should read the consent request carefully as it may limit their rights. A customer may maintain their consent preferences, including their marketing preferences, at any time. A customer can maintain their consent preferences, including their marketing preferences (by giving or withdrawing the consent) on the group apps or websites, or through cellphone banking, contact centres or branches. The customer can also contact the responsible parties as listed in section 5.

**NOTE:** As the group has operations in several countries, this notice will apply to the processing of personal information by any entity in the group in any country. The processing of customers’ personal information may be

conducted outside the borders of South Africa, but will be processed according to the requirements and safeguards of applicable privacy law or privacy rules that bind the group. If a group entity has its own notice, that notice would take precedence over this notice.

## 5 RESPONSIBLE PARTIES

The group has several responsible parties. These companies are responsible for determining why and how the group will use customers' personal information. When a customer uses the group's platform, the responsible party would be the company within the group that provides the platform, acting jointly with the other companies in the group. Similarly, when a customer uses a solution provided by any group entity, the responsible party will be the entity which the customer engages to take up the solution, acting jointly with the other entities in the group.

Customers can contact the various responsible parties in the group through the applicable business, the email addresses of which are listed below.

|   |                                |
|---|--------------------------------|
|    | fnbpaia@fnb.co.za              |
|  | rmbprivacy.office@rmb.co.za    |
|  | wesbankpaia@wesbank.co.za      |
|  | firstrandcosec@firstrand.co.za |
|  | fnbpaia@fnb.co.za              |
|  | compliance@motovantage.co.za   |

## 6 CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL INFORMATION BY THE BANKING INDUSTRY

FirstRand Bank Limited (the bank), is a registered bank in South Africa and a member of the Banking Association South Africa (BASA). As a BASA member, the bank is subject to the Code of Conduct for the Processing of Personal Information by the Banking Industry (the code). The bank will process customers' personal information in terms of the code. A copy of the code can be found on the respective bank website.

## 7 WHAT IS PERSONAL INFORMATION?

Personal information refers to any information that identifies a customer or specifically relates to a customer. Personal information includes, but is not limited to, the following information about a customer:

| Birth (e.g. date of birth)   | Education  | Language  | Age  |
|--|--|---|--|
| National origin  | Marital status (e.g. married, single, divorced)                                  | Financial history (e.g. income; expenses; financial obligations; assets and liabilities; buying, investing, lending, insurance, banking and money management behaviour; goals and needs) based on, among others, account transactions | Employment history and current employment status (e.g. when a customer applies for credit) |
| Gender or sex (e.g. for statistical purposes as required by the law)   | Identifying number (e.g. an account number, identity number or passport number)  | Email address, physical address (e.g. residential address, work address or physical location), telephone number   | Information about a customer's location (e.g. geolocation or GPS location)                 |
| Online identifiers (e.g. cookies, online analytical identifier numbers, internet protocol (IP) addresses, device fingerprints, device ID), social media profiles | Biometric information (e.g. fingerprints, signature, facial biometrics or voice) | Race (for statistical purposes as required by the law)  | Religion, belief, conscience, culture  |
| Physical health, mental health, wellbeing, disability  | Employment history   | Criminal history  | Medical history (e.g. HIV/Aids status)   |
| Personal views, preferences and opinions   | Confidential correspondence  | Views or opinions about a customer  | Customer's name  |

Depending on the applicable law of the country, a juristic entity (like a company) may also have personal information, which is protected by law and which may be processed in terms of this notice.

There is also a category of personal information called **special personal information**, which is considered more sensitive and is afforded additional protection in the law. Special personal information includes the following personal information about a customer:

|   |  |               |                        |
|---|--|---------------|------------------------|
| Religious and philosophical beliefs (e.g. where a customer enters a competition and is requested to express a philosophical view) | Race (e.g. where a customer applies for a solution where the statistical information must be recorded) | Ethnic origin | Trade union membership |
|---|--|---------------|------------------------|

|                   |   |  |  |
|-------------------|---|--|--|
| Political beliefs | Health, including physical or mental health, disability and medical history (e.g. where a customer applies for an insurance policy) | Biometric information (e.g. to verify a customer's identity) | Criminal behaviour where it relates to the alleged commission of any offence or the proceedings relating to that offence |
|-------------------|---|--|--|

## 8 WHEN WILL THE GROUP PROCESS CUSTOMERS' PERSONAL INFORMATION?

The group may process customers' personal information for lawful purposes relating to its business if the following circumstances apply:

- it is necessary to conclude or perform under a **contract** the group has with the customer or to provide a solution to the customer;
- the **law** requires or permits it;
- it is required to protect or pursue the customer's, the group's or a third party's **legitimate interest**;
- the customer has **consented** thereto;
- a person legally authorised by the customer, the law or a court, has consented thereto; or
- the customer is a child and a competent person (such as a parent or guardian) has consented thereto on their behalf.

## 9 WHEN WILL THE GROUP PROCESS CUSTOMERS' SPECIAL PERSONAL INFORMATION?

The group may process customers' special personal information in the following circumstances, among others:

- if the processing is needed to create, use or protect a right or obligation in **law**;
- if the processing is for **statistical or research** purposes, and specific conditions set in applicable privacy laws are met;
- if the special personal information was made **public** by the customer;
- if the processing is required by **law**;
- if racial information is processed and the processing is required to **identify** the customer;
- if health information is processed, and the processing takes place to determine a customer's **insurance** risk, to perform under an insurance policy, or enforce an insurance right or obligation; or
- if the customer has **consented** to the processing.

## 10 WHEN AND HOW WILL THE GROUP PROCESS THE PERSONAL INFORMATION OF CHILDREN?

*A child is a person who is defined as a child by a country's legislation, and who has not been recognised as an adult by the courts.*

The group processes the personal information of children if the law permits this.

If a customer gives the group the personal information of a child the customer confirms that the customer is permitted to act on behalf of the child and agrees to the processing of the child's personal information in terms of this notice.

The group may process the personal information of a child if any one or more of the following applies:

- a person with the ability to sign legal agreements has **consented** to the processing, e.g. the parent or guardian of the child;
- the processing is needed to create, use or protect a right or obligation in **law**, such as where the child is an heir in a will, a beneficiary of a trust, a beneficiary of an insurance policy or an insured person in terms of an insurance policy;
- the child's personal information was made **public** by the child, with the consent of a person who can sign legal agreements;
- the processing is for **statistical or research** purposes and all legal conditions are met;
- where the child is legally old enough to open a **bank account** without assistance from their parent or guardian;
- where the child is legally old enough to sign a document as a **witness** without assistance from their parent or guardian; or
- where the child benefits from a bank account such as an investment or savings account and a person with the ability to sign legal agreements has consented to the processing.

## 11 WHEN AND FROM WHERE DOES THE GROUP OBTAIN PERSONAL INFORMATION ABOUT CUSTOMERS?

The group collects information about customers:

- directly from customers;
- based on the customers' use of the group's platform (e.g. behavioural information derived from interaction and movements on the group's platform);
- based on customers' use of group solutions or service channels (like group websites, applications (apps) and ATMs, including both assisted (with help) and unassisted (without help) customer interactions);
- based on how customers engage or interact with the group, such as on social media, and through emails, letters, telephone calls and surveys;
- based on a customer's relationship with the group;
- from public sources (newspapers, company registers, online search engines, deed registries, public posts on social media and public directories);
- from technology, such as a customer's access and use, including both assisted and unassisted interactions (e.g. on the group's websites and mobile apps) to access and engage with the group's platform (this includes cookies and online or app analytics);
- customers' engagement with group advertising, marketing and public messaging; and
- from parties that the group interacts with when conducting its business (approved business partners who are natural or juristic persons holding a business relationship with the group, where such relationship does not fall within the category of a supplier, employee or customer relationship, and where the relationship exists to offer customers assets, insurance products or other value-added solutions, such as insurers; original equipment manufacturers and dealers; reward partners; list providers, marketing list or lead providers; the group's customer loyalty rewards programmes' retail and online partners; credit bureaux; regulators and government departments or service providers).

The group collects and processes customers' personal information at the start of and for the duration of their relationship with the group. The group may also process customers' personal information when their relationship with the group has ended.

If the law requires the group to do so, it will ask for customer consent before collecting personal information about them from other parties.

The parties (which may include parties the group engages with as independent responsible parties, joint responsible parties or operators) from whom the group may collect customers' personal information include, but are not limited to, the following:

- members of the group, any connected companies, subsidiary companies, its associates, cessionaries, delegates, assignees, affiliates or successors in title and/or appointed parties (such as its authorised agents, partners, contractors and suppliers) for any of the purposes identified in this notice;
- the financial services and product providers within the group, including representatives and intermediaries;
- the customer's spouse; dependants; partners; employer; joint applicant, account or card holder; authorised signatories or mandated persons; beneficiaries and other similar sources;
- people whom the customer has authorised to share their personal information, such as a person that makes a travel booking on their behalf or a medical practitioner for insurance purposes;
- attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements;
- payment processing service providers, merchants, banks and other persons that assist with the processing of customers' payment instructions, such as card scheme providers (including Visa or Mastercard);
- insurers, brokers, other financial institutions or other organisations that assist with insurance and assurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims, and other related purposes;
- law enforcement and fraud prevention agencies, and other persons tasked with the prevention and prosecution of crime;
- regulatory authorities, industry ombuds, government departments, and local and international tax authorities;
- credit bureaux;
- financial services exchanges;
- qualification information providers;
- trustees, executors or curators appointed by a court of law;
- payment or account verification service providers;
- the group's service providers, agents and subcontractors, such as couriers and other persons the group uses to offer and provide solutions to customers;
- courts of law or tribunals;
- participating partners, whether retail or online, of the group's customer rewards programmes;
- the group's joint venture partners;
- the group's business partners;
- marketing list or lead providers;
- social media platforms;
- the user of a SIM card who is not the subscriber of the SIM card, where telecommunication services are provided; or
- online search engine providers.

Important: If the customer provides the group with personal information of other people the customer confirms that the customer is allowed to share it with the group and that the group may process the personal information in terms of this notice.

## 12 REASONS THE GROUP NEEDS TO PROCESS CUSTOMERS' PERSONAL INFORMATION

The group may process customers' personal information for the reasons outlined below.

### 12.1 Contract

The group may process customers' personal information if it is necessary to conclude or perform under a contract the group has with a customer, provide a solution to a customer or manage interactions with customers on the platform service channels and interfaces. This includes:

- to assess and process applications for solutions;
- to assess the group's lending and insurance risks;
- to conduct affordability assessments, credit assessments and credit scoring;
- to conduct a needs analysis so that the correct solution meeting the customer's needs and circumstances may be provided;
- to provide a customer with solutions they have requested;
- to open, manage and maintain customer accounts or relationships with the group;
- to enable the group to deliver goods, documents or notices to customers;
- to communicate with customers and carry out customer instructions and requests;
- to respond to customer enquiries and complaints;
- to enforce and collect on any agreement when a customer is in default or breach of the terms and conditions of the agreement, such as tracing a customer, or instituting legal proceedings against a customer. In such a scenario the group may aggregate the contact details provided to any of the companies in the group to determine the customer's most accurate contact details to enforce or collect on any agreement the customer has with the group;
- to disclose and obtain personal information from credit bureaux regarding a customer's credit history;
- to meet record-keeping obligations;
- to conduct market and behavioural research, including scoring and analysis to determine if a customer qualifies for solutions, or to determine a customer's credit or insurance risk;
- to enable customers to participate in and make use of value-added solutions;
- to enable customers to participate in customer rewards programmes — to determine customer qualification for participation, their rewards level and their rewards points, and monitor customer buying behaviour with the group's rewards partners in order to allocate the correct points or inform customers of appropriate solutions they may be interested in, or to inform the group's reward partners about a customer's purchasing behaviour;
- to enable the sale and purchase of and payment for goods in the group's digital marketplaces;
- to make travel bookings, payments and arrangements;
- to conduct customer satisfaction surveys and promotional and other competitions;

- to enable insurance and assurance underwriting and administration;
- to process, consider and assess insurance or assurance claims;
- to provide insurance and assurance policies, products and related services;
- to conduct security and identity verification, and to check the accuracy of customer personal information;
- to provide telecommunication, data and SIM card products and services;
- to provide information in compliance with the group's obligations relating to funding, financing and credit rating agreements; and
- for any other related purposes.

## 12.2 Law

The group may process customers' personal information if the law requires or permits it. A schedule of legislation which requires the group to process personal information is included on page 29 of this notice. The group may process customers' personal information:

- to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules);
- to comply with voluntary and involuntary codes of conduct and industry agreements;
- to ensure that customers are treated fairly and to comply with conduct standards issued by market conduct authorities, which include the identification or determination, recording and appropriate treatment of customer vulnerabilities like adverse life events;
- to fulfil reporting requirements and information requests;
- to process payment instruments and payment instructions (such as a debit order);
- to create, manufacture and print payment instruments and payment devices (such as a debit card);
- to meet record-keeping obligations;
- to detect, prevent and report theft, fraud, money laundering, corruption and other crimes. This may include the processing of special personal information, such as alleged criminal behaviour, the supplying of false, misleading or dishonest information when opening an account with the group or avoiding liability by way of deception, to the extent allowable under applicable privacy laws. The Financial Intelligence Centre Act obliges the group to collect personal and special personal information from customers and other parties, to process personal and special personal information and further process personal and special personal information for financial crime detection, prevention and reporting. The processing of personal information and special personal information may happen when customers transact, establish a relationship with the group and use group solutions;
- to assist public bodies (like government departments and entities) to perform their public law duties, including disclosure, verification, validation and sharing of customer personal information to detect, prevent, report and monitor fraud and other crimes and to meet Financial Action Task Force requirements and obligations;
- to conduct market and behavioural research, including scoring and analysis to determine if a customer qualifies for solutions, or to determine a customer's credit or insurance risk;

- to enable customers to participate in and make use of value-added solutions (e.g. the payment of traffic fines or renewal of vehicle licences);
- to enable customers to participate in customer rewards programmes by determining customer qualification for participation, their rewards level and points, and to monitor customer buying behaviour with the group's rewards partners to allocate the correct points or inform customers of appropriate solutions they may be interested in, or to inform the group's reward partners about a customer's purchasing behaviour;
- for customer satisfaction surveys, and promotional and other competitions;
- to assess the group's lending and insurance risks;
- to conduct affordability assessments, credit assessments and credit scoring;
- to disclose and obtain personal information from credit bureaux regarding a customer's credit history;
- to develop credit models and credit tools;
- for insurance and assurance underwriting and administration;
- to process, consider or assess insurance or assurance claims;
- to provide insurance and assurance policies and products, and related services;
- to give effect to and adhere to legislation governing various protected relationships (e.g. civil unions, marriages or customary marriages);
- to calculate contributions and coverage, make payment of contributions and report personal information of qualifying depositors, deposits and products to the Corporation for Deposit Insurance in terms of deposit insurance regulations;
- environmental, social and governance (ESG) reporting; or
- for any other related purposes

### **12.3 Legitimate interest**

The group may process customers' personal information in the daily management of its business and finances and to protect the group's customers, employees, service providers and assets. It is to the group's and its customers' benefit to ensure that its procedures, policies and systems operate efficiently and effectively.

The group may process customers' personal information to provide them with the most appropriate solutions, and to develop and improve group solutions, group business and the group's platform. This includes communicating with customers about these solutions.

The group may process a customer's personal information if it is required to protect or pursue their, the group's or a third party's legitimate interests. These include:

- to develop, implement, monitor and improve the group's business processes, policies and systems;
- to manage business continuity and emergencies;
- to protect and enforce the group's rights and remedies in the law;
- to develop, test and improve solutions for customers, which may include connecting customer personal information with other personal information obtained from parties or public records to better understand customer needs and develop solutions that meet these needs. The group may also consider customer actions, behaviour, preferences, expectations, feedback and financial history;

- to tailor solutions which would include consideration of a customer's use of third-party products, goods and services and to market appropriate solutions to the customer, including marketing on the group's own or other websites, mobile apps and social media;
- to market group solutions to customers via various means, including on group and other websites and mobile apps including social media, as well as tele-, postal and in-person marketing;
- to market business partner solutions via various means;
- to respond to customer enquiries and communications including the recording of engagements and analysing the quality of the group's engagements with a customer;
- to respond to complaints including analytics of complaints to understand trends and prevent future complaints and provide compensation where appropriate;
- to enforce and collect on any agreement when a customer is in default or breach of the terms and conditions of the agreement, such as tracing the customer or instituting legal proceedings against the customer. In such a scenario, the group may aggregate the contact details provided to any of the companies in the group to determine the customer's most accurate contact details to enforce or collect on any agreement the customer has with the group;
- to process payment instruments and payment instructions (such as a debit order);
- to create, manufacture and print payment instruments and payment devices (such as a debit card);
- to meet record-keeping obligations;
- to fulfil reporting requirements and information requests;
- to comply with voluntary and involuntary codes of conduct and industry agreements;
- to detect, prevent and report theft, fraud, money laundering, corruption and other crimes. This may include the processing of special personal information, such as alleged criminal behaviour or the supplying of false, misleading or dishonest information when opening an account with the group, or avoiding liability by way of deception, to the extent allowable under applicable privacy laws. This may also include the monitoring of the group's buildings by means of, for example, CCTV cameras and access control;
- to assist public bodies (like government departments and entities) to perform their public law duties, including disclosure, verification, validation and sharing of customer personal information to detect, prevent, report and monitor fraud and other crimes and to meet Financial Action Task Force requirements and obligations;
- to conduct market and behavioural research, including scoring and analysis to determine if a customer qualifies for solutions, or to determine a customer's credit or insurance risk;
- for statistical purposes, such as market segmentation or customer segments (placing customers in groups with similar customers based on their personal information);
- to enable customers to participate in customer rewards programmes by determining customer qualification for participation, their rewards level and points, and by monitoring customer buying behaviour with the group's rewards partners to allocate the correct points or inform customers of appropriate solutions they may be interested in, or to inform the group's reward partners about a customer's purchasing behaviour;
- for customer satisfaction surveys and promotional and other competitions;

- to assess the group’s lending and insurance risks;
- to disclose and obtain personal information from credit bureaux regarding a customer’s credit history;
- to develop credit models and credit tools;
- for purposes of ESG reporting;
- to provide information in compliance with the group’s obligations relating to funding, financing and credit rating agreements; or
- for any other related purposes.

### 13 WHY DOES THE GROUP FURTHER USE OR PROCESS CUSTOMERS’ PERSONAL INFORMATION?

At the time that the group collects personal information from a customer, it will have a reason or purpose to collect that personal information, which includes all the purposes disclosed in this notice. The group may use that same personal information for other purposes. The group will only do this where the law allows it to and where the other purposes are compatible with the original purpose(s) applicable when the group collected the customer’s personal information as disclosed in this notice. Examples of these other purposes are included in the list of purposes set out in section 12 above.

The group may also need to request a customer’s specific consent for further processing in limited circumstances.

The group may also further use or process a customer’s personal information if:

- the personal information about the customer was obtained from a **public** record, such as a deeds registry;
- the customer made the personal information public, for example on social media;
- the personal information is used for **historical, statistical** or **research** purposes and the results will not identify the customer;
- proceedings have started or are contemplated in a **court** or **tribunal**;
- it is in the interest of **national security**;
- it is necessary to prevent or reduce a serious and imminent **threat** to public health or public safety;
- it is necessary to prevent or reduce a serious and imminent **threat** to the **life** or **health** of a person including our customers (for example, engaging law enforcement agencies or medical providers and provide personal information to help);
- if the group is required to adhere to the **law**, specifically tax legislation; or
- the Information Regulator has **exempted** the processing.

The group may also further use or process a customer’s personal information if the customer has consented to it, or in the instance of a child, if a competent person has consented to it.

Any enquiries about the further processing of customer personal information can be made through the contact details of the customer’s solution provider or the group’s platform provider, as set out in the responsible parties table in section 5 of this notice.

## 14 CENTRALISED PROCESSING

The group aims to create efficiencies in the way it processes information across the group. Customers' personal information may therefore be processed through centralised group functions and systems, which include the housing of personal information in centralised group data warehouses.

This centralised processing is structured to ensure efficient processing that benefits both the customer and the group. Such benefits include, but are not limited to:

- improved information management, integrity and information security;
- the leveraging of centralised crime and fraud prevention tools. This would include the processing of the customer's personal information and special personal information across the companies in the group to prevent, detect and report on financial crimes and related matters in terms of the Financial Intelligence Centre Act;
- improved knowledge of a customer's financial service needs so that appropriate solutions can be advertised and marketed to the customer;
- a reduction in information management costs;
- analytics, statistics and research, and
- streamlined transfers of personal information for customers with solutions across different businesses or companies within the group.

Details of further interests which are promoted by the centralised processing can be found in section 12.

**VERY IMPORTANT:** If customers use the group's platform, group solutions or service channels and interfaces (including both assisted (with help) and unassisted (without help) interactions), or by accepting any rules, agreements, contracts, mandates or annexures with the group, or by utilising any solutions offered by the group, customers agree to:

- conclude and fulfil contractual terms or obligations to a customer;
- comply with obligations imposed by law; or
- protect or pursue customers', the group's or a third party's legitimate interests, including designing, offering and communicating solutions that best meet customers' needs.

Customers' personal information may be processed through centralised functions and systems across companies in the group and may be used for the purposes, in the manner and with the appropriate controls as set out in this notice.

## 15 ENRICHING PERSONAL INFORMATION

The group aims to provide its customers with solutions that are appropriate and reasonable considering the customer's circumstances (such as financial position (including income, deductions and expenses), employment status and various obligations), vulnerabilities and needs.

The group may not always have sufficient personal information (obtained from companies within the group or from the customer) about the customer to determine the suitability of solutions applied for, to determine which solutions are appropriate to offer proactively to customers or to assist customers with money management tips

and advice. In these circumstances, the group may approach external persons for additional personal information.

The group may get, use and share within the group customer personal information (such as what customers purchase and spend their money on, which insurance and investment products customers have and how customers meet their obligations under these products, whether customers have medical aid and how they are meeting their obligations regarding the medical aid, and what customers' salaries are) from the following entities in South Africa:

- retailers (including physical and online retailers like grocery, convenience, clothing and speciality retailers);
- telecommunication service providers (including those that provide or distribute airtime and data);
- long-term and short-term insurance providers (including the product suppliers, the intermediaries and the brokers);
- investment providers (including asset managers);
- the customer's bank; and
- customer employers and payroll management companies for customer employers.

The purposes for which customer personal information may be used are:

- To determine creditworthiness when applying for credit (which includes the validation of sources of income and income amounts) and to proactively provide suitable credit solutions.
- To manage the credit solutions held with the group.
- To underwrite long-term or short-term insurance policies when customers apply for them and to proactively provide customers with suitable insurance solutions.
- To prevent, detect and report fraud and other crimes, which includes protecting customers and the group against fraud and other crimes.
- To offer and provide customers with suitable group solutions, including credit, insurance, investment, transaction and value-added solutions.
- To place customers in the correct customer segment and therefore improve financial and non-financial guidance to customers from the group.

## **16 HOW DOES THE GROUP USE CUSTOMERS' PERSONAL INFORMATION FOR REWARDS?**

The group collects personal information about customers from the partners; suppliers; customer loyalty rewards programmes' retail, online and strategic partners (rewards partners) and service providers it interacts with in relation to its eBucks rewards programme.

The group will process customers' personal information for the following reasons:

- to determine customer qualification for participation in the eBucks rewards programme and allocation of rewards points, rewards level and benefits;
- to inform the group's reward partners about customers' purchasing behaviour and to monitor customer buying behaviour with the group's rewards partners to correctly allocate eBucks earned;

- to provide rewards and benefits tailored to customer requirements and to treat customers in a more personalised manner;
- to fulfil customers' travel arrangements (flights, hotels and car hire) bookings with the group's service providers and deliver the solutions they have asked for;
- to fulfil customers' eBucks shop or similar purchases and instruct the group's service providers to deliver the solutions the customer has requested;
- to fulfil customers' requests for services provided by the group's reward partners and/or the group's service providers;
- to market the group's rewards and the group's rewards partners' solutions to customers;
- to market vehicle-related solution offers from the group or its business partners;
- to improve the group's websites, apps, solutions and rewards offerings;
- to respond to customer enquiries and complaints;
- to comply with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules);
- to comply with voluntary and involuntary codes of conduct and industry agreements;
- to fulfil reporting requirements and information requests;
- to conduct market and behavioural research, including scoring and analysis to determine if a customer qualifies for rewards, benefits and solutions;
- to develop, test and improve rewards and solutions for customers;
- for statistical purposes, such as market segmentation;
- to communicate with customers and carry out their instructions and requests;
- to conduct customer satisfaction surveys, promotional and other competitions; or
- for any other related purposes.

## **17 HOW DOES THE GROUP USE PERSONAL INFORMATION FOR DIRECT MARKETING?**

The group would like to keep its customers informed on solutions that may be of benefit to them. The group may use prospective customers' or customers' personal information to directly market financial and non-financial solutions to them.

The group aims to enhance the customer experience when using the group's platform. In order to do so, the group processes customer personal information to provide customers with personalised and appropriate offers that may be of interest to them. These personalised and appropriate offers are part and parcel of the group's platform and cannot be removed. If a customer does not want to receive these offers, they are requested to not use the group's platform.

### **WHO IS A GROUP CUSTOMER AND WHAT DOES THE TERM MEAN?**

For the purposes of electronic marketing (such as SMS, MMS, email, instant messaging or app notifications) and applicable to this section only, a group customer would be a person whose contact details were obtained during a sale of the group's solutions, including an instance where the person agrees to a solution being provided to them and the group not charging for that solution; where the person started to apply or register for a solution but decided to not continue or cancelled the transaction; if the group or the person declined the offer of a solution

made to or by the person; and where the person concluded an agreement with the group regarding the solution offered to them.

The group will use the personal information of these customers to communicate information about the group's financial solutions.

If a customer uses the group's platform, solutions or service channels and interfaces, or accepts any rules, agreements, contracts, mandates or annexures with the group, or uses any solutions offered by the group, the customer agrees to the processing by the group of their personal information for direct marketing of financial solutions (this includes transactional, lending, investment, insurance and related solutions).

If a person is a prospective customer (not a group customer) or in any other instances where the law requires, the group will only market to them by electronic communications with their consent.

### **IMPORTANT: HOW TO OPT OUT**

A customer may maintain their consent preferences, including direct marketing consent preferences, on the group's platform at any time. Details on how to change customer information and marketing preferences are available on the various group apps and websites. A customer can maintain their consent preferences (by giving or withdrawing their consent) by means of the group apps, websites, cellphone banking, contact centres or branches, or by contacting the responsible parties as per section 5.

For example: This can be done on the FNB app under My profile >My preferences >Marketing preferences and >Information preferences.

This section only applies to direct marketing by the group. It does not apply to other communications, including:

- communications with customers required by law;
- communications with customers required by contracts;
- operational communications (e.g. whether a premise is relocating);
- communications to protect customers (e.g. security tips);
- communications to customers about solutions they already hold with the group and how to best use and manage the solutions; and
- communications to customers about the group's platform and its service channels and interfaces.

## **18 WHEN WILL THE GROUP USE CUSTOMERS' PERSONAL INFORMATION TO MAKE AUTOMATED DECISIONS ABOUT THEM?**

An automated decision is made when a customer's personal information is analysed without human intervention in the decision-making process.

The group may use a customer's personal information to make an automated decision as allowed by law. An example of automated decision-making is the approval or declining of a credit application when a customer applies for an overdraft or credit card, or the approval or declining of an insurance claim.

Customers have the right to query any such decisions made, and the group will:

- provide the customer with sufficient information about the personal information which was used as well as how and why the group arrived at the decision; and
- inform the customer of processes available to enable them to make representations relating to the automated decision-making and provide them with a reasonable opportunity to make representations to the group.

## **19 WHEN, HOW AND WITH WHOM DOES THE GROUP SHARE CUSTOMERS' PERSONAL INFORMATION?**

In general, the group will only share customers' personal information if any one or more of the following apply:

- if the customer has **consented** to this;
- if it is necessary to conclude or perform under a **contract** the group has with the customer;
- if the **law** requires it; or
- if it is necessary to protect or pursue the customer's, the group's or a third party's **legitimate interest**.

Where permitted, each entity in the group may share a customer's personal information with the following persons, which may include parties that the group engages with as independent responsible parties, joint responsible parties or operators. These persons must keep customers' personal information secure and confidential:

- other group entities, any connected companies, subsidiary companies, associates, cessionaries, delegates, assignees, affiliates or successors in title and/or appointed parties (such as its authorised agents, partners, contractors and suppliers) for any of the purposes identified in this notice;
- the providers of financial services and products providers, including representatives and intermediaries;
- the group's employees, as required by their employment conditions;
- the customer's spouse; dependants; partners; employer; joint applicant, account or card holder; authorised signatories or mandated persons; beneficiaries and other similar sources;
- people the customer has authorised to obtain their personal information, such as a person who makes a travel booking on the customer's behalf, or a medical practitioner for insurance purposes;
- attorneys, tracing agents, debt collectors and other persons who assist with the enforcement of agreements;
- payment processing service providers, merchants, banks and other persons who assist with the processing of customer payment instructions, such as card scheme providers (including VISA or MasterCard);
- insurers, brokers and financial institutions or other organisations that assist with insurance and assurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims, and other related purposes;

- law enforcement and fraud prevention agencies, and other persons tasked with the prevention and prosecution of crime;
- regulatory authorities, industry ombuds, government departments, local and international tax authorities and other persons the law requires the group to share customer personal information with;
- credit bureaux;
- financial services exchanges;
- qualification information providers;
- trustees, executors or curators appointed by a court of law;
- payment or account verification service providers;
- the group's service providers, agents and subcontractors, such as couriers and other persons the group uses to offer and provide solutions to customers;
- persons to whom the group has ceded its rights or delegated its obligations under agreements, such as where a business is sold;
- courts of law or tribunals that require personal information to adjudicate referrals, actions or applications;
- the general public, where customers submit content to group social media sites such as a group business's Facebook page;
- participating partners in the group's customer reward programmes, where customers purchase products and services or spend loyalty rewards;
- the user of a SIM card who is not the subscriber of the SIM card, where telecommunication services are provided; or
- the group's joint venture or business partners with which it has concluded business agreements.

## **20 WHEN AND HOW DOES THE GROUP OBTAIN CUSTOMERS' PERSONAL INFORMATION FROM CREDIT BUREAUX AND WHEN WILL IT SHARE CUSTOMERS' PERSONAL INFORMATION WITH CREDIT BUREAUX?**

The group may obtain customers' personal information from credit bureaux for any one or more of the following reasons:

- if the customer requested the group to do so, or agreed that it may do so;
- to verify a customer's identity;
- to obtain or verify a customer's employment details;
- to obtain and verify a customer's marital status;
- to obtain, verify, or update a customer's contact or address details;
- to obtain a credit report about a customer which includes their credit history and credit score, when the customer applies for an agreement, a debt obligation or a credit agreement to prevent reckless lending or over-indebtedness;
- to determine a customer's credit risk;
- for debt recovery;
- to trace a customer's whereabouts;
- to update a customer's contact details;
- to conduct research, statistical analysis or system testing;
- to determine the source(s) of a customer's income;
- to build credit scorecards which are used to evaluate credit applications;
- to set the limit for the supply of an insurance policy;
- to assess the application for insurance coverage;
- to obtain a customer's contact details to enable the distribution of unclaimed benefits under an insurance policy; or

- to determine which solutions to promote or offer to a customer.

The group will share a customer's personal information with credit bureaux for, among others, any one or more of the following reasons:

- to report the application for an agreement, debt obligation or credit agreement;
- to report the opening of an agreement, debt obligation or credit agreement;
- to report the termination of an agreement, debt obligation or credit agreement;
- to report payment behaviour on an agreement, debt obligation or credit agreement; or
- to report non-compliance with an agreement, debt obligation or credit agreement, such as not paying in full or on time.

Customers should refer to their specific credit agreement with the group for further information.

## 21 UNDER WHICH CIRCUMSTANCES WILL THE GROUP TRANSFER CUSTOMERS' PERSONAL INFORMATION TO OTHER COUNTRIES?

The group will only transfer a customer's personal information to third parties in another country in any one or more of the following circumstances:

- where a customer's personal information 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 the customer or a contract with a third party that is in the customer's interest;
- where the customer has **consented** to the transfer; or
- where it is not reasonably practical to obtain the customer's consent, but the transfer is in the **customer's interest**.

This transfer will happen within the requirements and safeguards of applicable laws or privacy rules that bind the group.

Where possible, the party processing a customer's personal information in another country will agree to apply the same level of protection as available by law in the customer's country, or if the other country's laws provide better protection, the other country's laws would be agreed to and applied.

An example of the group transferring a customer's personal information to another country would be when a customer makes payments if they purchase goods or services in a foreign country, or where personal information is stored with a cloud services provider and the servers are in a foreign country.

**TAKE NOTE:** As the group operates in several countries, customers' personal information may be shared with group companies in other countries and processed in those countries under the privacy rules that bind the group.

## 22 CUSTOMERS' DUTIES AND RIGHTS REGARDING THE PERSONAL INFORMATION THE GROUP HOLDS ABOUT THEM

Customers must provide the group with proof of identity when enforcing the rights below. The group will then verify the identity of the customer. Customers must inform the group when their personal information changes, as soon as possible after the change.

**IMPORTANT:** Customers warrant that, when they provide the group with personal information regarding their spouse, dependants or any other person, they have permission from them to share their personal information with the group. The group will process the personal information of the customer's spouse, dependant or any other person that the customer has shared with it as stated in this notice.

### 22.1 Right to access

Customers have the right to request access to the personal information the group has about them by contacting the group. This includes requesting:

- confirmation that the group holds the customer's personal information;
- a copy or description of the record containing the customer's personal information; and
- the identity or categories of third parties who have had access to the customer's personal information.

The group will address requests for access to personal information within a reasonable time and in alignment with the law. Customers may be required to pay a reasonable fee (aligned with the law) to receive copies or descriptions of records of, or information on, third parties. The group will inform customers of the fee before attending to their request.

Customers should note that the law may limit their right to access information, e.g. information relating to the group's intellectual property, competitively sensitive information or legally privileged information.

For South Africa, please refer to the group's information manual prepared under section 51 of the Promotion of Access to Information Act, No. 2 of 2000 (information manual) for further information on how customers can effect this right. The information manual is available on the group's website at: <https://www.firststrand.co.za/media/investors/policies-and-practice/pdf/firststrand-information-manual.pdf>.

In certain instances, customers exercise this right by making use of the group's unassisted (self-help) interfaces, e.g. using a group entity's app or website to access the personal information the group holds about them (for example, on the FNB app under My profile).

### 22.2 Right to correction, deletion or destruction

Customers have the right to request the group to correct, delete or destroy the personal information it has about them if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully, or if the group is no longer authorised to keep it. Customers must inform the group of their request in the prescribed form. Prescribed form 2 has been included as an annexure to this notice.

The group will take reasonable steps to determine if the personal information is correct and make any corrections needed. It may take a reasonable time for the change to reflect on the group's platform/systems. The group may request documents from the customer to verify the change in personal information.

A specific agreement that a customer has entered into with the group may determine how they must amend their personal information provided at the time when they entered into the specific agreement. Customers are required to adhere to these requirements.

If the law requires the group to retain the personal information, it will not be deleted or destroyed upon the customer's request. The deletion or destruction of certain personal information may lead to the termination of a customer's relationship with the group.

The group may be unable to establish a relationship with a customer, continue a relationship with a customer, process a transaction or provide a customer with a solution if the customer withholds or requests the deletion of personal information or special personal information required in terms of the Financial Intelligence Centre Act for financial crime prevention, detection and reporting purposes.

In certain instances a customer can give effect to this right by making use of the group's unassisted (self-help) interfaces, e.g. using a group app or website to correct their contact details.

### **22.3 Right to objection**

Customers may object to the processing of their personal information on reasonable grounds where the processing is in their legitimate interest, the group's legitimate interest or in the legitimate interest of another party.

Customers must inform the group of their objections in the prescribed form. Prescribed form 1 is included as an annexure to this notice.

The group will not be able to give effect to the customer's objection if the processing of their personal information was and is permitted by law, the customer has provided consent to the processing and the group's processing was conducted in line with their consent; or the processing is necessary to conclude or perform under a contract with the customer.

The group will also not be able to give effect to a customer's objection if the objection is not based upon reasonable grounds and substantiated with appropriate evidence.

The group will provide customers with feedback regarding their objections.

### **22.4 Right to withdraw consent**

Where a customer has provided their consent for the processing of their personal information, the customer may withdraw their consent. If they withdraw their consent, the group will explain the consequences to the customer. If a customer withdraws their consent, the group may not be able to provide certain solutions to the customer or provide the customer access to the group's platform. The group will inform the customer if this is the case. The group may proceed to process customers' personal information, even if they have withdrawn their consent, if

the law permits or requires it. It may take a reasonable time for the change to reflect in the group's systems. During this time, the group may still process the customer's personal information.

**IMPORTANT: HOW TO WITHDRAW CONSENT**

A customer may maintain their consent preferences, including direct marketing consent preferences, at any time on the group's platform. Details on how to change customer information and marketing preferences are available on the various group apps and websites. A customer can maintain their consent preferences (by giving or withdrawing the consent) by means of group apps, websites, cellphone banking, contact centres or branches, or by contacting the responsible parties as per section 5.

For example this can be done on the FNB app under My profile >My preferences >Marketing preferences and >Information preferences.

**22.5 Right to complain**

Customers have a right to file a complaint with the group or any regulator with jurisdiction (in South Africa customers can contact the Information Regulator) about an alleged contravention of the protection of their personal information. The group will address customer complaints as best possible.

The contact details of the Information Regulator are provided below.

|  |  |   |
|--|--|---|
| Physical address:  | Postal address:  |   |
| JD House, 27 Stiemens Street<br>Braamfontein<br>Johannesburg<br>2001 | P.O. Box 31533<br>Braamfontein<br>Johannesburg<br>2017 | Telephone number: +27 (0)10 023 5200<br>Website: <a href="https://info regulator.org.za">https://info regulator.org.za</a><br>Complaints email address:<br>POPIAComplaints@info regulator.org.za<br>General enquiries email address:<br>enquiries@info regulator.org.za |

FirstRand Bank Limited, a registered bank in South Africa and a member of the Banking Association South Africa, is subject to the Code of Conduct for the Processing of Personal Information by the Banking Industry. As such, privacy complaints may be referred to:

**National Financial Ombud Scheme South Africa**

|   |  |   |
|---|--|---|
| NFO Johannesburg<br>110 Oxford Road<br>Houghton Estate<br>Johannesburg<br>Gauteng<br>2198 | NFO Cape Town<br>Claremont Central Building<br>6th Floor<br>6 Vineyard Road, Claremont<br>Western Cape<br>7700 | Telephone number: 0860-800-900<br>Website: <a href="http://www.nfosa.co.za/">http://www.nfosa.co.za/</a><br>Email address: <a href="mailto:info@nfosa.co.za">info@nfosa.co.za</a> |
|---|--|---|

## 22.6 Right to Legal Action

Customers have the right to take legal action, and in South Africa, request that the Information Regulator take legal action, for certain contraventions of the protection of their personal information.

## 23 HOW THE GROUP SECURES CUSTOMERS' PERSONAL INFORMATION

The group will take appropriate and reasonable technical and organisational steps to protect customers' personal information in line with industry best practices. The group's security measures, including physical, technological and procedural safeguards, will be appropriate and reasonable. This includes the following:

- keeping group systems secure (such as monitoring access and usage);
- storing group records securely;
- controlling access to group premises, systems and/or records; and
- safely destroying or deleting records.

Customers can also protect their personal information and can obtain more information in this regard by visiting the website or app of the relevant group entity that they have established a relationship with.

## 24 HOW LONG DOES THE GROUP KEEP CUSTOMERS' PERSONAL INFORMATION?

The group will keep customers' personal information for as long as:

- the **law** requires the group to keep it;
- a **contract** between the customer and the group requires the group to keep it;
- the customer has **consented** to the group keeping it;
- the group is required to keep it to achieve the **purposes** listed in this notice;
- the group requires it for **statistical or research** purposes;
- a **code of conduct** requires the group to keep it; and/or
- the group requires it for **lawful business purposes**.

**TAKE NOTE:** The group may retain customers' personal information even if they no longer have a relationship with the group or if they request the group to delete or destroy it, if the law permits or requires it.

Please refer to the FirstRand group cookie notice for further information. The group's cookie notice is available on FirstRand's website.

## 25 HOW THE GROUP PROCESSES PERSONAL INFORMATION ABOUT PERSONS RELATED TO A JURISTIC PERSON

If a customer is a juristic person, such as a company or close corporation, the group may collect and use personal information relating to the juristic person's directors, officers, employees, beneficial owners, partners, shareholders, members, authorised signatories, representatives, agents, payers, payees, customers, guarantors, spouses of guarantors, sureties, spouses of sureties, other security providers and other persons related to the juristic person. These are related persons.

If customers provide the personal information of a related person to the group, they warrant that the related person is aware that they are sharing their personal information with the group, and that the related person has consented thereto.

The group will process the personal information of related persons as stated in this notice. Therefore references to “customer(s)” in this notice will include related persons with the necessary amendments and limitations.

## **26 CESSION, DELEGATION OR ASSIGNMENT**

The companies in the group may cede, delegate or assign fully or partially their rights and obligations under this notice to another company. This assignment may take place without customer consent. Personal information related to a customer of the company may also be transferred to the other company. The other company will adhere to all privacy laws, all privacy undertakings the group has given and all processing and marketing consent preferences the customer has provided to the group (including opt-ins and opt-outs). The group will provide the customer with notification of this transfer of personal information.

## **27 CHANGES TO THIS NOTICE**

The group may change this notice from time to time. The updated notice will become operative when published on the group’s websites. The latest version of the notice displayed on FirstRand’s website will apply to customers’ interactions with the group and the group’s processing of the customers’ personal information. It is available at <https://www.firstrand.co.za/investors/esg-resource-hub/policies-and-practices/>.

## 28 ANNEXURES

- **FORM 1:**

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 2]

- **FORM 2**

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 3]

## 29 SCHEDULE OF LEGISLATION

The group may process a customer's personal information where the processing is required, permitted or contemplated in law. Below is a list of legislation which requires the group to process the personal information of customers. The list of legislation should be read to include all related subordinate legislation thereunder.

- Administration of Estates Act 66 of 1965
- Banks Act 94 of 1990
- Bribery Act 2010 (United Kingdom)
- Broad-based Black Economic Empowerment Act 53 of 2003
- Collective Investment Schemes Control Act 45 of 2002
- Competition Act 89 of 1998
- Common Reporting Standards
- Companies Act 71 of 2008
- Conduct Standard 3 of 2020 (BANKS)
- Consumer Protection Act 68 of 2008
- Criminal Finances Act 2017 (United Kingdom)
- Currency and Exchanges Act 9 of 1933
- Cybercrimes Act 19 of 2020
- Data Protection (Bailiwick of Guernsey) Law, 2017
- Disaster Management Act 57 of 2002
- Electronic Communications Act 36 of 2005
- Electronic Communications and Transactions Act 25 of 2002
- Estate Duty Act 45 of 1955
- Financial Advisory and Intermediary Services Act 37 of 2002
- Financial Institutions (Protection of Funds) Act 28 of 2001
- Financial Intelligence Centre Act 38 of 2001
- Financial Markets Act 19 of 2012
- Financial Sector Regulation Act 9 of 2017
- Foreign Account Tax Compliance Act (United States)
- Foreign Corrupt Practices Act of 1977 (United States)
- Immigration Act 13 of 2002
- Insurance Act 18 of 2017
- JSE Equities Rules and Equities Directives
- JSE Limited Listing Requirements
- Long-term Insurance Act 52 of 1998
- Modern Slavery Act 2015 (United Kingdom)
- National Credit Act 34 of 2005
- National Payment System Act 78 of 1998
- Pension Funds Act 24 of 1956
- Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004
- Protection of Personal Information Act 4 of 2013
- Prevention and Combating of Corrupt Activities Act 12 of 2004
- Prevention and Combating of Trafficking in Persons Act 7 of 2013
- Prevention of Organised Crime Act 121 of 1998
- Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
- Short-term Insurance Act 53 of 1998
- Trust Property Control Act 57 of 1988