FNB ESWATINI CUSTOMER PRIVACY NOTICE

March 2025

Version 2.0

TABLE OF CONTENTS

1 DEFINITIONS 3
2 BACKGROUND AND PURPOSE OF THIS NOTICE 3
3 WHAT IS PERSONAL INFORMATION? 5
4 WHEN WILL FNB PROCESS CUSTOMERS' PERSONAL INFORMATION? 6
5 WHEN WILL FNB PROCESS CUSTOMERS' SPECIAL PERSONAL INFORMATION? 6
6 WHEN AND HOW WILL FNB PROCESS THE PERSONAL INFORMATION OF CHILDREN? 6
7 WHEN, AND FROM WHERE, DOES FNB OBTAIN PERSONAL INFORMATION ABOUT CUSTOMERS? 10
8 REASONS FNB NEEDS TO PROCESS CUSTOMERS' PERSONAL INFORMATION 0
9 WHY DOES FNB FURTHER USE OR PROCESS CUSTOMERS' PERSONAL INFORMATION? 2
10 CENTRALISED PROCESSING 3
11 HOW DOES FNB USE CUSTOMERS' PERSONAL INFORMATION FOR REWARDS? 4
12 HOW FNB USES PERSONAL INFORMATION FOR MARKETING? 5
13 WHEN WILL FNB USE CUSTOMERS' PERSONAL INFORMATION TO MAKE AUTOMATED DECISIONS ABOUT THEM? 5
14 WHEN, HOW, AND WITH WHOM DOES FNB SHARE CUSTOMERS' PERSONAL INFORMATION? 6
15 WHEN AND HOW FNB OBTAINS AND SHARES CUSTOMERS' PERSONAL INFORMATION FROM/WITH CREDIT BUREAUX? 7
16 UNDER WHAT CIRCUMSTANCES WILL FNB TRANSFER CUSTOMERS' PERSONAL INFORMATION TO OTHER COUNTRIES? 8
17 CUSTOMERS' DUTIES AND RIGHTS REGARDING THE PERSONAL INFORMATION FNB HAS ABOUT THEM 9
18 HOW FNB SECURES CUSTOMERS' PERSONAL INFORMATION 11
19 HOW LONG DOES FNB KEEP CUSTOMERS' PERSONAL INFORMATION? 11
20 COOKIES 12
21 HOW FNB PROCESSES PERSONAL INFORMATION ABOUT PERSONS RELATED TO A JURISTIC PERSON 12
22 CHANGES TO THIS NOTICE 13
ANNEXURES 14

1 DEFINITIONS

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

For the purpose of this notice a "customer" includes:

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

What Is "Process"?
In this notice "process" means how FNB collects, uses, stores, makes available, destroys, updates, discloses or otherwise deals with customers' personal information.

What is a "Data Controller"?
A person who alone or together with others, determines the purpose of and means for processing personal information, regardless of whether or not such data is processed by that party or by a data processor on its behalf, where the purpose and means of processing are determined by law

The data controller will be FNB, which from an overall perspective determines the purpose and means for processing personal information.

What is a "Data Processor"?
A person that 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 data controller

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

2 BACKGROUND AND PURPOSE OF THIS NOTICE

Protecting customers' personal information is important to FNB. To do so, it follows general principles in accordance with applicable privacy laws.

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

FNB collects personal information about its customers. This includes what customers tell FNB about themselves, what FNB learns by having a customer or when a customer makes use of a solution or interacts with FNB's platform through various interfaces and channels, as well as the choices customers make about the marketing they elect to receive. This notice also outlines customers' privacy rights and how the law protects customers.

In terms of applicable privacy laws, this notice may also apply on behalf of other third parties (such as authorised agents and contractors), acting on FNB's behalf when providing customers with solutions.

FNB respects customers' privacy and will treat their personal information confidentially.

FNB may combine customers' personal information (across FNB's platform, interfaces or channels and use the combined personal information for any of the purposes stated in this notice.

VERY IMPORTANT: If customers use FNB's platform, solutions or service channels (including both assisted and unassisted interactions), or by accepting any rules, agreement, contract, mandate or annexure with FNB, or by utilising any solutions offered by FNB, customers agree that in order to:

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

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

Where it is necessary to obtain consent for processing, FNB will seek customers' consent separately. Customers should read the consent request carefully as it may limit their rights. A customer may maintain their consent preferences on FNB's platform. Customers can go to branch to change their preferences.

NOTE: This notice will apply to the processing of personal information by FNB, and the processing of customers' personal information may be conducted outside the borders of Eswatini but will be processed according to the requirements and safeguards of applicable privacy law or privacy rules that bind FNB. If FNB processes personal information for another party under a contract or a mandate, the other party's privacy notice will apply to the processing.

FNB may change this notice from time to time if required by law or its business practices. Where the change is material, FNB will notify customers and will allow a reasonable period for customers to raise any objections before the change is made. Please note that FNB may not be able to continue a relationship with a customer or provide customers with certain solutions or permit access to FNB's platform if they do not agree to the changes.

The latest version of the notice displayed on FNB Eswatini's website will apply to customers' interactions with FNB and is available at: https://www.fnbswaziland.co.sz/legal/privacyPolicy.html.

3 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:

- marital status (married, single, divorced); national origin; age; language; birth; education;
- financial history (e.g. income, expenses, obligations, assets and liabilities or buying, investing, lending, insurance, banking and money management behaviour or goals and needs based on, amongst others, account transactions);
- employment history and current employment status (for example when a customer applies for credit);
- gender or sex (for statistical purposes as required by the law);
- identifying number (e.g. an account number, identity number or passport number);
- e-mail 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);
- physical health; mental health; wellbeing; disability; religion; belief; conscience; culture;
- medical history (e.g. HIV/AIDS status); criminal history; employment history;
- personal views, preferences and opinions;
- confidential correspondence; or
- another's views or opinions about a customer and a customer's name also constitute personal information.

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

There is also a category of personal information called **special personal information**, which includes the following personal information about a customer:

- religious and philosophical beliefs (for example 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); or

- criminal behaviour where it relates to the alleged commission of any offence or the proceedings relating to that offence.

4 WHEN WILL FNB PROCESS CUSTOMERS' PERSONAL INFORMATION?

FNB 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 FNB has with the customer or to provide the solution to the customer;
- the law requires or permits it;
- it is required to protect or pursue the customer's, FNB'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.

5 WHEN WILL FNB PROCESS CUSTOMERS' SPECIAL PERSONAL INFORMATION?

FNB 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 all legal conditions 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 is to determine a customer's insurance risk, or to perform under an insurance policy, or to enforce an insurance right or obligation; or
- if the customer has consented to the processing.

6 WHEN AND HOW WILL FNB PROCESS THE PERSONAL INFORMATION OF CHILDREN?

A child is a person who is defined as a child by the Children's Protection and Welfare Act, 2012, and who has not been recognised as an adult by the courts.

FNB processes the personal information of children if the law permits this.

FNB may process the personal information of children if any one or more of the following applies:

- a person with the ability to sign legal agreements has consented to the processing, being 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.

7 WHEN, AND FROM WHERE, DOES FNB OBTAIN PERSONAL INFORMATION ABOUT CUSTOMERS?

FNB collects information about customers:

- directly from customers;
- based on the customers' use of FNB's platform (e.g. behavioural information derived from interaction and movements on FNB's platform);
- based on customers' use of FNB solutions or service channels (such as FNB website, application (app) and ATMs, including both assisted and unassisted customer interactions) as applicable;
- based on how customers engage or interact with FNB, such as on social media, and through emails, letters, telephone calls and surveys;
- based on a customer's relationship with FNB;
- from public sources (such as newspapers, company registers, online search engines, deed registries, public posts on social media, public directories);
- from technology, such as a customer's access and use including both assisted and unassisted interactions (e.g. on FNB's website and mobile app) to access and engage with FNB's platform (this includes cookies and online or app analytics);
- customers' engagement with FNB advertising, marketing and public messaging; and
- from third parties that FNB interacts with for the purposes of conducting its business (such as approved business partners who are natural or juristic persons holding a business relationship with FNB, where such relationship does not fall within the category of a supplier, employee or customer relationship, e.g. insurers, original equipment manufacturers (OEMs) and dealers to offer customers assets, insurance products or other value-added solutions), reward partners, list providers, marketing list or lead providers, FNB's customer loyalty rewards programmes' retail and online partners, credit bureaux, regulators and government departments or service providers).

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

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

The third parties (which may include parties FNB engages with as independent data controllers, joint data controllers or processors) from whom FNB may collect customers' personal information include, but are not limited to, the following:

- members of FirstRand Limited (which includes First National Bank, WesBank, Rand Merchant Bank and FirstRand Limited), any connected companies, subsidiary companies, its associates, cessionaries, delegates, assignees, affiliates or successors in title and/or appointed third 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 FNB, 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 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 services 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;
- FNB's service providers, agents and subcontractors, such as couriers and other persons FNB uses to offer and provide solutions to customers;
- courts of law or tribunals;
- participating partners, whether retail or online, in FNB's customer rewards programmes;
- FNB's joint venture partners;
- FNB'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 FNB with personal information of other people, the customer confirms that the customer is allowed to share it with the bank and that the bank may process the personal information in terms of this notice.

8 REASONS FNB NEEDS TO PROCESS CUSTOMERS' PERSONAL INFORMATION

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

8.1 Contract

FNB may process customers' personal information if it is necessary to conclude or perform under a contract FNB has with a customer or to provide a solution to a customer. This includes:

- to assess and process applications for solutions;
- to assess FNB'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 FNB;
- to enable FNB 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 to institute legal proceedings against a customer. In such scenario FNB may aggregate the contact details provided to any of the companies in FNB to determine the customer's most accurate contact details in order to enforce or collect on any agreement the customer has with FNB;
- 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: determine customer qualification for participation, rewards points, rewards level, and monitor customer buying behaviour with FNB's rewards partners to allocate the correct points or inform customers of appropriate solutions they may be interested in, or to inform FNB's reward partners about a customer's purchasing behaviour;
- to enable the sale and purchase of and payment for goods in FNB's digital marketplaces;
- travel bookings, payments and arrangements;
- customer satisfaction surveys, promotional and other competitions;

- insurance and assurance underwriting and administration;
- to process or consider or assess insurance or assurance claims;
- to provide insurance and assurance policies, products and related services;
- security and identity verification, and to check the accuracy of customer personal information;

  or
- for any other related purposes.

8.2 Law

FNB may process customers' personal information if the law requires or permits it. This includes:

- 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;
- 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 or the supply of false, misleading or dishonest information when opening an account with FNB, or avoiding liability by way of deception, to the extent allowable under applicable privacy laws. The Money Laundering and Financing of Terrorism (Prevention) Act obliges FNB to collect personal and special personal information from customers and other third parties, to process personal and special personal information and further process personal and special personal information for the purposes of financial crime detection, prevention and reporting. The processing of personal information and special personal information may happen when customers transact, establish a relationship with FNB and when utilising FNB 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 law enforcement agencies 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, renewal of vehicle licences, etc.);
- to enable customers to participate in customer rewards programmes: determine customer qualification for participation, rewards points, rewards level, and monitor customer buying behaviour with FNB's rewards partners to allocate the correct points or inform customers of appropriate solutions they may be interested in, or to inform FNB's reward partners about a customer's purchasing behaviour;

- for customer satisfaction surveys, promotional and other competitions;
- to assess FNB'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 or 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, customary marriages); or
- for any other related purposes.

8.3 Legitimate interest

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

FNB may process customers' personal information to provide them with the most appropriate solutions and to develop and improve the bank solutions, business and its platform.

FNB may process a customer's personal information if it is required to protect or pursue their, FNB's or a third party's legitimate interest. This includes:

- to develop, implement, monitor and improve FNB's business processes, policies and systems;
- to manage business continuity and emergencies;
- to protect and enforce FNB's rights and remedies in the law;
- to develop, test and improve solutions for customers, this may include connecting customer personal information with other personal information obtained from third parties or public records to better understand customer needs and develop solutions that meet these needs. FNB may also consider customer actions, behaviour, preferences, expectations, feedback and financial history;
- tailoring solutions which would include consideration of a customer's use of third-party products, goods and services and marketing of appropriate solutions to the customer, including marketing on FNB's own or other websites, mobile apps and social media;
- to market FNB solutions to customers via various means including on FNB 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 FNB's engagements with a customer;
- to respond to complaints including analytics of complaints to understand trends and prevent future complaints and providing 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 to institute legal proceedings against the customer. In such a scenario, FNB may aggregate the contact details provided to any of the companies in FNB to determine the customer's most accurate contact details in order to enforce or collect on any agreement the customer has with FNB;
- 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 supply of false, misleading or dishonest information when opening an account with FNB, or avoiding liability by way of deception, to the extent allowable under applicable privacy laws. This may also include the monitoring of FNB's buildings including 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 law enforcement agencies 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 (that is placing customers in groups with similar customers based on their personal information);
- to enable customers to participate in customer rewards programmes: determine customer qualification for participation, rewards points, rewards level, and monitor customer buying behaviour with FNB's rewards partners to allocate the correct points or inform customers of appropriate solutions they may be interested in, or to inform FNB's reward partners about a customer's purchasing behaviour;
- for customer satisfaction surveys, promotional and other competitions;
- to assess FNB'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 any other related purposes.

9 WHY DOES FNB FURTHER USE OR PROCESS CUSTOMERS' PERSONAL INFORMATION?

At the time that FNB 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. In certain circumstances, however, FNB may use that same personal information for other purposes. FNB will only do this where the law allows it to and the other purposes are compatible with the original purpose/s applicable when FNB collected the customer's personal information. FNB may also need to request a customer's specific consent for the further

processing in limited circumstances. Examples of these other purposes are included in the list of purposes set out in section 8 above.

FNB may also further use or process a customer's personal information if:

- the personal information about the customer was obtained from a public record, like the deed's registry;
- the customer made the personal information public, like on social media;
- the personal information is used for historical, statistical or research purposes, 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 FNB must adhere to the law, specifically tax legislation; or
- the Commission has exempted the processing.

FNB 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, a parent (or competent person) has consented to it.

Any enquiries about the further processing of customer personal information can be made through the bank's Customer Service Centre (CSC), through the toll-free 8006100 or email to gethelp@fnb.co.sz.

10 CENTRALISED PROCESSING

FNB as a subsidiary of FirstRand Group, aims to create efficiencies in the way it processes information. Customers' personal information may therefore be processed through centralised group functions and systems, which includes the housing of their personal information in a centralised group data warehouse.

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 your 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 Money Laundering and Financing of Terrorism (Prevention) Act.
- better 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 8.3.

Should a customer wish to exercise their privacy rights in terms of personal information provided to the bank or enquire about the centralised processing procedure, enquiries can be made through the bank's Customer Service Centre (CSC), through the toll-free 8006100 or email to gethelp@fnb.co.sz.

11 HOW DOES FNB USE CUSTOMERS' PERSONAL INFORMATION FOR REWARDS?

FNB collects personal information about customers from its partners, suppliers, customer loyalty rewards programmes' retail, online and strategic partners (rewards partners) and service providers with which FNB interacts for the purposes of its rewards programme.

FNB will process customers' personal information for the following reasons:

- to determine customer qualification for participation in the rewards programme, rewards points, rewards level and benefits;
- to inform FNB's reward partners about customers' purchasing behaviour and to monitor customer buying behaviour with FNB's rewards partners to correctly allocate points earned;
- to provide rewards and benefits tailored to customer requirements and to treat customers in a more personal way;
- to fulfil customers' travel arrangements (flights, hotels and car hire) bookings with FNBs' service providers and deliver the solutions they have asked for;
- to fulfil customers' requests for services provided by FNB's reward partners and/or FNB's service providers;
- to market FNB's rewards and FNB's rewards partners' solutions to customers;
- to market vehicle-related solution offers from Wesbank;
- to improve FNB's website, app, 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;
- for customer satisfaction surveys, promotional and other competitions; or
- for any other related purposes.

12 HOW FNB USES PERSONAL INFORMATION FOR MARKETING?

- FNB may use prospective customers' or customers' personal information to market financial, insurance, investments and other related banking and other financial solutions to them.
- FNB will do this in person, by post, telephone, or electronic channels such as SMS, email or app notifications.
- If a person is a prospective customer (not a FNB customer) or in any other instances where the law requires, FNB will only market to them by electronic communications with their consent.
- **For the purposes of electronic marketing and this paragraph only**, a FNB customer would be a person whose contact details were obtained in the context of the sale of FNB's solutions, including:
  - where the person agrees to a solution being provided to them and FNB does not charge for that solution;
  - where the person started to apply or register for a solution but decided to not continue or cancel the transaction;
  - if FNB or the person declined the offer of a solution made to or by the person; and
  - where the person concluded an agreement with FNB regarding the solution offered to the person.
- In all cases, a person can request FNB to stop sending marketing communications to them at any time.
- The person can also withdraw marketing consent or opt-out of marketing at any time. FNB has various interfaces and channels that can be used to withdraw marketing consent or opt-out of marketing, e.g. for example, FNB's branches.

13 WHEN WILL FNB 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 that decision-making process.

FNB may use a customer's personal information to make an automated decision as allowed by the 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 FNB will:

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

14 WHEN, HOW, AND WITH WHOM DOES FNB SHARE CUSTOMERS' PERSONAL INFORMATION?

In general, FNB 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 FNB has with the customer;
- if the law requires it; or
- if it is necessary to protect or pursue the customer's, FNB's or a third party's legitimate interest.

Where permitted, FNB may share a customer's personal information with the following persons, which may include parties that FNB engages with as independent data controllers, joint data controllers or data processors. These persons have an obligation to keep customers' personal information secure and confidential:

- other FirstRand Limited entities, any connected companies, subsidiary companies, associates, cessionaries, delegates, assignees, affiliates or successors in title and/or appointed third parties (such as its authorised agents, partners, contractors and suppliers) for any of the purposes identified in this notice;
- the financial services and products providers in FNB, including representatives and intermediaries;
- FNB's employees, as required by their employment conditions;
- the customer's spouse, dependants, partners, employer, joint applicant or account or card holders, authorised signatories or mandated persons, beneficiaries and other similar sources;
- people the customer has authorised to obtain their personal information, such as a person that makes a travel booking on the customer's 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 services providers, merchants, banks and other persons that assist with the processing of customer 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 and other persons the law requires FNB 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;

- FNB's service providers, subcontractors, such as couriers and other persons FNB uses to offer and provide solutions to customers;
- persons to whom FNB have ceded its rights or delegated its obligations to under agreements, such as where a business is sold;
- courts of law or tribunals that require the personal information to adjudicate referrals, actions or applications;
- the general public, where customers submit content to the bank's social media sites such as a FNB business's Facebook page;
- participating partners in FNB'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
- FNB's joint venture and business partners with which it has concluded business agreements.

15 WHEN AND HOW FNB OBTAINS AND SHARES CUSTOMERS' PERSONAL INFORMATION FROM/WITH CREDIT BUREAUX?

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

- if the customer requested FNB 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 cover;
- 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 to offer to a customer.

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

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

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

Below is the contact detail of the credit bureaux that FNB interacts with:

- TransUnion ITC Swaziland (Pty) Ltd (+268) 2505 7844

16 UNDER WHAT CIRCUMSTANCES WILL FNB TRANSFER CUSTOMERS' PERSONAL INFORMATION TO OTHER COUNTRIES?

FNB 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; and/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 FNB.

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 Eswatini, or if the other country's laws provide better protection, the other country's laws would be agreed to and applied.

An example of FNB 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 FNB is a subsidiary of FirstRand Limited which operates in several countries, customers' personal information may be shared with the group companies in other countries and processed in those countries under the privacy laws that bind FNB and FirstRand Limited.

17 CUSTOMERS' DUTIES AND RIGHTS REGARDING THE PERSONAL INFORMATION FNB HAS ABOUT THEM

Customers must provide FNB with proof of identity when enforcing the rights below and FNB will then verify the identity of the customer.

Customers must inform FNB when their personal information changes, as soon as possible after the change.

Customers warrant that when they provide FNB with personal information of their spouse, dependants or any other person, they have permission from them to share their personal information with FNB. FNB will process the personal information of the customer's spouse, dependent or any other person which the customer has shared with it as stated in this notice.

17.1 Right to access

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

- confirmation that FNB 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.

FNB will attend to 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 to the law) to receive copies or descriptions of records, or information about, third parties. FNB 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 FNB's intellectual property, competitively sensitive information or legally privileged information.

In certain instances, customers can give effect to this right by making use of FNB's unassisted interfaces, e.g. using FNB's app or website to access the personal information FNB holds about them.

17.2 Right to correction, deletion or destruction

Customers have the right to request FNB 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 FNB are no longer authorised to keep it. Customers must inform FNB of their request in the prescribed form. Prescribed form 2 has been included as an annexure to this notice.

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

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

If the law requires FNB to keep 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 FNB.

FNB may not be able 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 withhold or request deletion of personal information or special personal information required in terms of The Money Laundering and Financing of Terrorism (Prevention) Act for financial crime prevention, detection and reporting purposes.

In certain instances, a customer can give effect to this right by making use of FNBs' unassisted interfaces, e.g. using a FNB app or website to correct their contact details.

17.3 Right to objection

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

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

FNB 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 FNB's processing was conducted in line with their consent; or the processing is necessary to conclude or perform under a contract with the customer.

FNB 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.

FNB will provide customers with feedback regarding their objections.

17.4 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, FNB will explain the consequences to the customer. If a customer withdraws their consent, FNB may not be able to provide certain solutions to the customer or provide the customer access to FNB's platform. FNB will inform the customer if this is the case. FNB 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 on FNBs' systems. During this time, FNB may still process the customer's personal information.

Customers can give effect to this right by making use of FNB's unassisted service channels, e.g. using a FNB app or website, or through an assisted interaction to update their consent preferences.

17.5 Right to complain

Customers have a right to file a complaint with FNB or any regulator with jurisdiction (in Eswatini customers can contact the Eswatini Communications Commission (ESCCOM)) about an alleged contravention of the protection of their personal information. FNB will address customer complaints as far as possible.

The contact details of the Eswatini Communications Commission (ESCCOM) are provided below.

Physical address	Plot 11/850, Mantenga Drive, Ezulwini
Postal address	PO Box 7811 Mbabane H100 Eswatini
Telephone number	+268 2406 7000
Website	https://www.esccom.org.sz https://edpa.org.sz
Complaints form	https://edpa.org.sz/Complaint.php
General enquiries email	info@esccom.org.sz

18 HOW FNB SECURES CUSTOMERS' PERSONAL INFORMATION

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

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

Customers can also protect their own personal information and can obtain more information in this regard by visiting the FNB website https://www.fnbswaziland.co.sz/.

19 HOW LONG DOES FNB KEEP CUSTOMERS' PERSONAL INFORMATION?

FNB will keep customers' personal information for as long as:

- the law requires FNB to keep it;
- a contract between the customer and FNB requires FNB to keep it;

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

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

20 COOKIES

A cookie is a small piece of data that is sent (usually in the form of a text file) from a website to the user's device, such as a computer, smartphone or tablet. There are different types of cookies which serve different purposes, and this is fully explained in the FNB cookie notice available on FNB's website. The purpose of a cookie is to provide a reliable mechanism to "remember" user behaviour (keeping track of previous actions), e.g. remembering the contents of an online shopping cart, and actions the user performed whilst browsing when not signed up or logged into their online account.

FNB does not necessarily know the identity of the user of the device but does see the behaviour recorded on the device. Multiple users of the same device would not necessarily be distinguishable from one another. Cookies could, however, be used to identify the device and, if the device is linked to a specific user, the user would also be identifiable. For example, a device registered to an app will be linked to the user.

By using FNB website or app, customers agree that cookies may be forwarded from the relevant website or app to their computer or device. Certain cookies will enable FNB to know that a customer has visited a website or app before and will identify the customer. FNB may also use third-party or necessary cookies to prevent fraud.

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

21 HOW FNB PROCESSES PERSONAL INFORMATION ABOUT PERSONS RELATED TO A JURISTIC PERSON

If a customer is a juristic person, such as a company or close corporation, FNB 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 FNB, they warrant that the related person is aware that they are sharing their personal information with FNB, and that the related person has consented thereto.

FNB will process the personal information of related persons as stated in this notice, thus references to "customer/s" in this notice will include related persons with the necessary amendments and limitations.

22 CHANGES TO THIS NOTICE

The bank may change this notice from time to time. The updated notice will become operative when published on the bank's websites. The latest version of the notice displayed on FNB's website will apply to customers' interactions with the bank and the bank's processing of the customers' personal information. It is available at https://www.fnbswaziland.co.sz/legal/privacyPolicy.html.

ANNEXURES

- **FORM 1:**

  OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 9 OF THE DATA PROTECTION ACT, 2022.

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

Note:
1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3. Complete as is applicable.

A	**DETAILS OF DATA SUBJECT** *(person who is objecting to the processing of his/her information)*		
Names and surname			
Unique Identifier / Identity Number / Unique government identifier			
Residential, postal or business address			
	Code ( )		
Contact number(s)		Fax number / E-mail address	
B	**IF THE OBJECTION IS IN RELATION TO PROCESSING ACTIVITIES PERFORMED BY A THIRD PARTY ON BEHALF OF THE BANK, THEN COMPLETE PART B**		
Name(s) and surname / registered name of third party			

C	**REASONS FOR OBJECTION** *(Please provide detailed reasons for the objection)*

Signed at _____ on _____ 20 _____

_____

Signature of data subject/designated person

- **FORM 2**

  REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 20 OF THE DATA PROTECTION ACT, 2022

FORM 2

REQUEST FOR CORRECTION, UPDATING, DELETION OR DESTRUCTION OF PERSONAL INFORMATION

Note:
1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3. Complete as is applicable.

Mark the appropriate box with an "X".
Request for:

☐ *Correction or updating of the personal information about the data subject.*

☐ *Destroying or deletion of a record of personal information about the data subject.*

A	**DETAILS OF DATA SUBJECT** *(person who is making this request regarding his/her information)*		
Names and surname			
Unique Identifier / Identity Number / Unique Government Identifier			
Residential, postal or business address			
	Code ( )		
Contact number(s)		Fax number / E-mail address	
B	**IF THE REQUEST IS IN RELATION TO PROCESSING ACTIVITIES PERFORMED BY SOMEONE OTHER THAN THE BANK (a third party), THEN COMPLETE PART B**		
Name(s) and surname / registered name of third party			

C	**INFORMATION TO BE DELETED/DESTROYED**
Information to be destroyed/deleted	
What information must be destroyed/deleted?	Why must the information be destroyed/delete?
D	**INFORMATION TO BE CORRECTED/UPDATED**
Information to be corrected/updated	
What information must be corrected/updated?	Why must the information be corrected/updated?

Signed at _____ on _____ 20 ____

_____

Signature of data subject/designated person