First National Bank

DATA PROTECTION POLICY FOR SUPPLIERS AND BUSINESS PARTNERS

POLICY LEVEL	First National Bank Ghana Ltd (FNBG)
NUMBER OF PAGES	13
RECOMMENDED BY	Compliance Department
APPROVED BY	FNBG Risk and Compliance Committee
LAST APPROVAL DATE	23rd April 2025
VERSION NUMBER	2.0
NEXT REVISION DATE	23rd April 2027

TABLE OF CONTENTS

Definition of terms used in this notice:

Affiliate	Means (a) any subsidiary or a holding company or a subsidiary of the holding company of either party, or (b) any entity that controls, is controlled by or is under common control with either party. The term "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of the entity through the ownership of voting securities representing 50% (fifty per cent) plus 1 (one) of the possible votes.
Agreement	Means the agreement entered into between the bank and the supplier or business partner, as applicable.
Information Regulator	Means the Information Regulator (eg, The Data Protection Commission) established in terms of the Data Protection Act 2012, Act 843
Business partner	A business partner, in the context of this policy, means a natural or juristic person (**person**) holding a business relationship with the bank, where such relationship does not fall within the category of a supplier, employee or customer relationship, and which person processes PI for, on behalf of or together with FNBG under the terms of the applicable agreement between the bank and the person. (*For the avoidance of doubt, the term **business partner** is used for the sake of convenience and for descriptive purposes only and should not be construed to imply a partnership between the bank and the business partner in a legal sense or as understood in law.)*
Child	A child is a natural person who is defined as a child by a country's legislation and who has not been recognised as an adult by the courts of a country.
Competent person	Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Consent	Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of PI.
Customer	A customer is a natural or legal person who is a First National Bank Ghana customer or a person who provided their PI/SPI to the bank in the context of a sale of acquiring goods or services.
Data subject	Means the person to whom PI relates. In reference to the bank, this primarily but without limitation means customers, employees and operators/suppliers, other persons and third parties.
Employee	Means a person employed for wages or a salary, including permanent employees, non-permanent employees, contractors, secondees and contingent workers.
Generative artificial intelligence (GAI)	Generative artificial intelligence refers to a category of artificial intelligence technology that generates new outputs based on the data it has been trained on. Unlike traditional artificial intelligence systems that are designed to recognise patterns and make predictions, generative artificial intelligence creates new content in the form of images, text, audio, and more.
Juristic person	Means an existing company, corporation, trust, not-for-profit organisation or other legal entity recognised by law as having rights and duties.
Legislation	Means relevant and applicable data privacy and protection legislation, including but not limited to: • the Data Protection Act 2012, Act 843.

Natural person	Means an identifiable, living human being.
Data processor	Means a person who processes PI for a Data Controller in terms of a contract or mandate, without coming under the direct authority of that Data Controller. This means any party that processes information on behalf of FNBG.
PCI standard	Means Payment Card Industry standard.
Personal information (PI)	Means information relating to an identifiable, living, (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other PI relating to the person or if the disclosure of the name itself would reveal information about the person. In reference to this policy, PI must be seen primarily but without limitation as PI of bank customers, employees and suppliers, and other persons and third parties.
PIN	Means "personal identification number", which is a secret numeric password known only to the user and a system to authenticate the user to the system.
DPA	Data Protection Act , 2012, Act 843
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning PI, including: (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
Public record	Means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
Record	Means any recorded information: (a) regardless of form or medium, including any of the following: (i) writing on any type of material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) a label, marking or other writing that identifies or describes anything of which it forms a part, or to which it is attached by any means; (iv) a book, map, plan, graph or drawing;

	(v) a photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) being in the possession of or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Data Controller	Means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. In reference to this Policy, a Data Controller would be a legal entity within FNBG that is registered and domiciled in Ghana or that is not domiciled in Ghana but makes use of automated or non-automated means in Ghana, to process personal information, and such processing extends beyond mere transmission of information through Ghana, and who determines the purpose and means for processing personal information, alone or in conjunction with others.
Sensitive cardholder PI	This information includes but is not limited to card validation codes/values, full track PI (from the magnetic strip or equivalent on a chip), PINs and PIN blocks. Authentication must be against cardholders and/or authorised payment card transactions in terms of PCI.
Special personal data	Means any PI of a data subject, concerning: (a) a child who is under parental control in accordance with the law, or (b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life of a data subject; (c) the criminal behaviour of a data subject to the extent that such information relates to: (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Supplier	Means a natural or juristic person who provides a product or renders services to the bank.
DEFINITIONS FROM THE GDPR	
Controller	Means a juristic person associated with First National Bank Ghana, registered in the United Kingdom, Guernsey or Jersey who, alone or jointly with others, determines the purposes and means for processing PI. Such purposes and means will be determined by the GDPR or privacy laws in the United Kingdom, Guernsey or Jersey.
Processor	Means a juristic person who processes PI on behalf of the controller.
Sub-processor	Means a juristic person defined in Annexures A1, A2 and A3 of this policy.

1 BACKGROUND AND PURPOSE OF THIS NOTICE

First National Bank Ghana Ltd (FNBG) (referred to as **the bank**) recognise that personal information (**PI**) and records are important assets that must be protected. This document establishes a governance framework that sets out ethical and sound PI protection practices that are to be followed by all suppliers and business partners appointed by the bank. This policy sets out the minimum PI protection requirements applicable to suppliers and business partners to preserve the integrity, confidentiality and availability of PI or records furnished to suppliers and business partners during the course and scope of their engagement with the bank.

Protecting the personal information of the bank's suppliers and business partners is important to FNBG. To do so, FNBG follows general principles in accordance with applicable privacy laws.
FNBG has developed this supplier and business partner privacy notice (**notice**) to enable its suppliers and business partners to understand how the bank collects, uses and safeguards their personal information.

This policy will set out the rules of engagement in relation to how PI is handled by suppliers and business partners on behalf of FNBG, as well as the minimum legal requirements that FNBG requires suppliers and business partners to adhere to, including compliance with the requirements of the Data Protection Act , 2012, Act 843 and other legislation, where applicable from time to time, in their capacity as service providers or business partners to the bank. This policy is applicable to all suppliers and applicable business partners who engage with the bank and handle PI as defined in applicable law.

All bank suppliers and business partners are expected to comply with Data Protection Act , 2012, Act 843

This policy serves as an additional measure which specifies the requirements that FNBG has in relation to how suppliers and business partners are required to organise themselves and provide goods and/or services or collaborate in relation to agreements concluded with FNBG and its affiliates.

FNBG subscribes to the higher of the host-or-home principle when dealing with jurisdictions outside of Ghana. This means that where the supplier or business partner conducts business activities within a jurisdiction where the PI protection laws and regulations are of a higher standard than Data Protection Act, 2012, Act 843, then the provisions of those laws and regulations will take precedence over the provisions of Data Protection Act, 2012, Act 843, and vice versa.

2 OWNERSHIP AND REVIEW

This policy is owned by FNBG Compliance and must be reviewed at least every two years. This policy will also be reviewed when any applicable code of conduct under Data Protection Act, 2012, Act 843 is published or there is any amendment to any overarching legislation.

3 RESPONSIBLE PARTIES

A **supplier**, in the context of this notice, means a natural or juristic person that provides a product or renders a service to the bank and is a data subject, where their personal information is processed by the bank. A supplier could also be considered a Data processor, an independent responsible party or (together with FNBG) a joint responsible party. The bank and its suppliers will always remain independent contracting parties.

A **business partner**, in the context of this notice, means a natural or juristic person holding a business relationship with the bank, where such relationship does not fall within the category of a supplier, employee or customer relationship. By virtue of the business relationship, FNBG may process personal information belonging to its business partner. Such a business partner is thus a data subject. For the avoidance of doubt, the term "business partner" is used for the sake of convenience and for descriptive purposes only. It should not be construed to imply a partnership between FNBG and the business partner in a legal sense or as understood in law. Depending on the nature of the business relationship, a business partner could be considered an operator, an independent responsible party or (together with FNBG) a joint responsible party. FNBG and its business partners will always remain independent contracting parties.

4 PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

Personal information refers to any information relating to the supplier or business partner which identifies the supplier or business partner (who can be a natural or a juristic person). If a supplier or business partner is a juristic person, the bank may collect and use personal information relating to the juristic person's directors, officers, employees, beneficial owners, partners, shareholders, members, subcontractors, 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 the suppliers' and business partners' related persons.

If the supplier or business partner provides FNBG with its related persons' personal information, the supplier or business partner warrants that the related persons are aware of and have consented to the sharing and processing of their personal information with/by FNBG. FNBG will process the personal information of related persons as stated in this notice. References to "the supplier" or "the business partner" in this notice will include related persons (with the necessary amendments).

Examples of the personal information of the supplier or business partner, where relevant, may include (but are not limited to):

- financial information of the supplier or business partner, which includes banking account information and financial records such as bank statements provided to the bank;
- invoices issued by the supplier or business partner to the bank;
- the contract/agreement between the bank and the supplier or business partner, including all annexures and addendums;
- other identifying information of the supplier or business partner, which includes company registration number, VAT number, tax number and contact details;
- marital status and matrimonial property regime (e.g. married in community of property);
- national origin;
- age;
- language;
- birth date;
- education;
- financial history;
- identifying number (e.g. an account number, identity number or passport number);
- information relating to political exposure;
- email address;
- physical address (e.g. residential address, work address or physical location);
- information about the location (e.g. geolocation or GPS location) of a supplier or business partner;
- telephone number;
- online and other unique identifiers;
- social media profiles;
- biometric information (like fingerprints, facial recognition signatures or voice collected through the bank's authenticated processes or CCTV);

- race;
- gender;
- sex;
- criminal history, personal views, preferences and opinions;
- confidential correspondence;
- another's views or opinions about a supplier or business partner; and/or
- the name of the supplier or business partner.

Some of the above personal information elements are considered special personal information, specifically as explained below.

Special personal data is personal information about the following:

- criminal behaviour, to the extent that such information relates to the alleged commission of an offence (for example to prevent money laundering as required by law, or to determine the desirability of entering into or maintaining a business relationship with the supplier or business partner), or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings;
- religious and philosophical beliefs (for example, where a supplier or business partner enters a competition and is requested to express a philosophical view);
- race or ethnic origin (e.g. for performing vendor and other risk management or statistical processes, including the determination and auditing of broad-based black economic empowerment status and levels);
- political beliefs (e.g. to determine political exposure and risk management for the purposes of anti-money laundering, anti-financial crime, anti-bribery and anti-corruption legislation);
- health, including physical or mental health, disability and medical history (e.g. when assessing eligibility for funding which may for example be in the form of grants or sponsorships, or when such information is collected via any one of the group's corporate and social responsibility initiatives); or
- biometric information (e.g. to verify identity and permit entry into the premises of the bank).

5 THE PURPOSES IN REFERENCE TO PROCESSING OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

Personal information will be processed by FNBG in the normal course of the management of suppliers and dealings with business partners for various purposes. Such purposes may include (where applicable to the relationship), but are not limited to:

- Procuring products, goods and services from the supplier or business partner.
- Responding to enquiries and complaints from the supplier or business partner.
- Maintaining the data of the supplier or business partner.
- Collaborating with the supplier or business partner (for example, collaborating in order to provide products or services to FNBG's customers).

- Complying with legislative, regulatory, risk and compliance requirements (including directives, sanctions and rules), voluntary and involuntary codes of conduct and industry agreements, or fulfilling reporting requirements and information requests.
- Detecting, preventing and reporting theft, fraud, money laundering and other crimes. This will include conducting criminal, credit reference/bureau, sanctions, anti-bribery and other related reference checks on the supplier or business partner, including but not limited to politically exposed persons (also known as PEP). Such checks may be conducted on an ongoing basis throughout the period of engagement, and may include lifestyle audits, forensic investigations relating to suspicions of misconduct (including whistle-blowing) and reporting on the conduct of suppliers or business partners to the relevant bodies before, after or during termination of the underlying agreement, where the bank is required to do so by law.
- To obtain personal information from credit bureaux regarding a supplier or business partner's credit history.
- Complying with all applicable laws authorising or requiring such processing,
- Enforcing and/or collecting on any agreement when the supplier or business partner is in default or breach of the agreement terms and conditions, e.g. tracing the supplier or business partner or instituting legal proceedings against the supplier or business partner.
- Conducting market and behavioural research, including scoring and analysis.
- Investigating and concluding on the outcome of matters referred to the independent ethics line (whistle-blowing), either by the supplier or business partner or about the supplier or business partner.
- Historical, statistical and research purposes, e.g. market segmentation or performance management.
- Security, identity verification and checking the accuracy of the personal information of the supplier or business partner.
- Performing vendor and other risk management processes.
- Communicating with the supplier or business partner and/or carrying out the instructions and requests of the supplier or business partner.
- Enabling the supplier's participation in supplier development programmes (including training and evaluation to access resources like funding and banking) and/or assessing the eligibility of the supplier or business partner for funding, which may for example be in the form of grants or sponsorships.
- Providing marketing or advertising to the supplier or business partner, in the context of supplier development programmes, while honouring consents and opt-outs.
- Generally exercising the bank's rights and carrying out FNBG's obligations in terms of the contract between the bank and the supplier or business partner.
- Any other related purposes.

FNBG will process a supplier's or a business partner's personal information pursuant to a lawful justification, including:

- the conclusion or performance of the contract to which the supplier or business partner is party or, prior to entering into the contract, taking the necessary steps to enable the negotiation and/or execution of the contract;
- compliance with legal obligations that the bank is subject to;
- the protection of a legitimate interest of the supplier or business partner; and/or
- the pursuit or maintenance of legitimate interests by the bank or by the third party to whom the personal information is disclosed for one or more of the above purposes.

There may be instances where the bank will lawfully process personal information for purposes not listed above. In this event, the bank may be required to request specific consent from the supplier or business partner, which consent may be withdrawn at any point.

6 THE CONSEQUENCES RELATING TO SUPPLIERS AND BUSINESS PARTNERS WHO DO NOT PROVIDE THEIR PERSONAL INFORMATION TO FNBG

In some circumstances, it may be mandatory for suppliers or business partners to provide their personal information. If a supplier or business partner refuses to provide the required personal information, the bank may be unable to carry out certain activities. For example, if a supplier or business partner refuses to provide the requisite personal information to enter into or pursue a contract or business relationship, the bank will be unable to enter into a contract or pursue any contractual relationship with the supplier or business partner.

7 THE QUALITY OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

FNBG will take reasonable and practicable steps to ensure that the personal information of the bank's suppliers and business partners is complete, accurate and not misleading, and is updated where necessary.

Suppliers and business partners can update their personal information, once given, by forwarding such a request to their contact person within the bank. The contact person will be the individual the supplier or business partner is working/dealing with from the bank.

8 SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

All personal information of the supplier or business partner processed by the bank will be held confidentially.

FNBG will take reasonable and appropriate technical and organisational measures to keep the personal information of its suppliers and business partners secure, in accordance with the group's policies and procedures on information security, and in accordance with any applicable law.

9 RETENTION OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

Personal information will not be kept by FNBG for longer than is necessary for the purposes of the processing set out above, unless a further retention period is required by law, or where FNBG reasonably requires a further retention period for a lawful purpose relating to its functions or activities, or where a further retention period is required by the contract between the supplier or business partner and FNBG, or where the retention is for historical, statistical or research purposes and appropriate safeguards have been applied to the personal information.

10 CENTRALISED PROCESSING

The bank aims to create efficiencies in the way it processes information across the bank. Suppliers' and business partners' personal information may therefore be processed through centralised functions and systems, which include storing

personal information in a centralised data warehouse, performing centralised administrative functions and providing a centralised payments system.

This centralised processing is structured to ensure efficient processing that benefits both the supplier or business partner and the bank. Such benefits include, but are not limited to:

- improved information management, integrity and information security;
- the leveraging of centralised crime and fraud prevention tools, which would include the processing of the supplier's and business partner's personal information and special personal information across the companies in the bank to prevent, detect and report on financial crimes and related matters in terms of the AML Act, Act 1044;
- a reduction in information management costs;
- analytics, statistics and research; and
- streamlined transfers of personal information for suppliers and business partners with solutions across different businesses or companies within the bank.

Should a supplier or business partner wish to exercise their privacy rights in terms of personal information provided to a company in the bank, or enquire about the centralised processing procedure, enquiries can be made through the contact details provided in this notice.

11 THE SHARING OF PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

The personal information of the supplier or business partner may be shared within FNBG and with affiliates and third parties with whom FNBG contracts in order to process such personal information pursuant to the instruction of FNBG, under specific terms or purposes as set out in this notice.

Moreover, certain affiliates and third parties could be based outside of Ghana. In such instances, and in other instances where it is necessary to transfer information outside of Ghana, FNBG will comply with cross-border transfer conditions of personal information as set out applicable legislations.

FNBG will ensure that reasonable and adequate safeguards are in place when sharing personal information of the supplier or business partner as set out above.

12 THE USE OF OPERATORS TO PROCESS PERSONAL INFORMATION PERTAINING TO SUPPLIERS AND BUSINESS PARTNERS

FNBG may assign the processing of the personal information of the supplier or business partner to an operator, who will process such personal information under a contract or mandate entered into with the bank. The operator may be a third party, another entity within the bank, an excluded subsidiary or an associate of the bank. In terms of a contract or mandate, FNBG will ensure that the operator processes the personal information of the supplier or business partner on a confidential basis and applies reasonable and appropriate technical and organisational security measures when processing the personal information of the supplier or business partner.

13 RIGHTS OF SUPPLIERS AND BUSINESS PARTNERS

Rights	Description of and information on the exercise of such rights
The right to be informed	This notice has been developed to enable suppliers and business partners to understand how the bank collects, uses and safeguards their personal information.
The right to access to information	A supplier or business partner has the right to access its personal information. A supplier or business partner may follow various avenues to access personal information. A supplier or business partner may contact FNBG or direct its request to the responsible relationship manager within the bank.
The right to the correction, destruction and deletion of and objection to the processing of the personal information of the supplier or business partner	Such requests can be sent to the responsible relationship manager within the bank. The responsible relationship manager will advise on the form and manner to submit and action such requests.
The right to object to direct marketing	If the personal information of the supplier or business partner has been used for direct marketing purposes, FNBG will afford the supplier or business partner (and the related persons of the supplier or business partner) an opportunity to opt out of receiving such direct marketing.
The right to withdraw consent	Where a supplier or business partner has provided their consent for the processing of their personal information, they may withdraw their consent. If they withdraw their consent, the bank will explain the consequences of such withdrawal.
The right to submit a complaint to FNBG and to the Information Regulator	Suppliers and business partners have the right to submit a complaint to the Information Regulator (Data Protection Commission of Ghana) regarding an alleged breach of the conditions for lawful processing of personal information. The contact details of the Data Protection Commission of Ghana is as below Website: https://dataprotection.org.gh support@dataprotection.org.gh Compliance: 0256302031, (030) 222-2929 Email address: info@dataprotection.org.gh Physical address: East Legon, Pawpaw Street, Ghana GPS: GA-414-1469
Right to Legal Action	Suppliers and business partners have the right to take legal action, and request that the Information Regulator take legal action, for certain contraventions of the protection of their personal information.

14 RESPONSIBILITIES OF SUPPLIERS AND BUSINESS PARTNERS WHO ARE OPERATORS

Where a supplier or business partner, in terms of a contract or mandate, processes personal information for responsible parties within the bank and is considered an operator of the bank, the supplier or the business partner must adhere to the obligations set out in the FNBG data protection policy for suppliers and business partners. This policy is available on the bank's website and sets out the rules of engagement in relation to how personal information is processed by suppliers and business partners on behalf of the bank, as well as the minimum legal requirements that FNBG requires the suppliers and business partners to adhere to in their capacity as suppliers or business partners to the bank. These include compliance with applicable legislations. This policy applies to all suppliers and business partners that engage with FNBG and handle personal information as defined in applicable law.

15 DOCUMENT INFORMATION

Any changes to this notice will come into force and effect once the updated notice has been published on the bank's websites.

-END-