BRANCH INTERNATIONAL FINANCE COMPANY LIMITED

DATA PROTECTION POLICY

March 2025

DATA PROTECTION POLICY	
DOCUMENT OWNER	Board of Directors
PREPARED BY	Legal and Compliance Team
REVIEW DATE	March 2025
NEXT REVIEW DATE	March 2028
VERSION	V2

Revision History

Version	Date	Revised By	Summary of Changes
2	March 2025	Jennifer Okwe Toluwase Omotehinse	1. Inclusion of Data Privacy Impact Assessment Procedure; 2. General update in compliance with the provisions of the Nigeria Data Protection Act (NDPA) 2023 and NDPA General Application and Implementation Directive (GAID) 2025.

TABLE OF CONTENTS

1. DEFINITIONS

"Automated Decision-Making" means a decision based solely on Automated Processing by automated means, without any human involvement;

"Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and deoxyribonucleic acid (DNA) analysis;

"Consent" means any freely given, specific, informed and unambiguous indication, whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or her or to another individual on whose behalf he has the permission to provide such consent;

"Data Controller" means an individual, private entity, public authority, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data;

"Data Processor" means an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of data controller or another data processor;

"Data Privacy Impact Assessment (DPIA)" means the process designed to identify the risks and impact of the envisaged processing of personal data. It comprises: a systematic description of the envisaged processing and its purpose including the legitimate interest pursued by the Data Controller, Data Processor, or third party; an assessment of the necessity and proportionality of the processing in relation to the purposes for which the personal data would be processed; an assessment of the risks to the rights and freedoms of the Data Subject; the measures identified to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data, taking into account the rights and legitimate interests of a Data Subject and other persons concerned;

"Data Protection Laws" means the Nigeria Data Protection Act (NDPA) 2023, NDPA General Application and Implementation Directive (GAID) 2025, and any other applicable data protection laws;

"Data Protection Officer (DPO)" means the person appointed as such under the Data Protection Laws and in accordance with its requirements. A DPO is responsible for advising Branch (including its employees) on their obligations under Data Protection Laws, monitoring compliance with Data Protection Laws, and Branch's policies;

"Data Subject" means an individual to whom personal data relates;

"Lawful Basis" means the basis for Processing Personal Data as set out in Paragraph 8 of this Policy;

"NDPA" means Nigeria Data Protection Act 2023;

"NDPA GAID" means Nigeria Data Protection Act General Application and Implementation Directive;

"**NDPC"or "Commission"** means Nigerian Data Protection Commission;

"Personal Data" means any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, psychological, genetic, physiological, cultural, social, or economic identity of that individual;

"Personal Data Breach" means a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"Policy" means this Data Protection Policy;

"Privacy by Design and Default" means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the NDPA by minimizing the risk factors that may exist as a result of engagement with Data Subjects, and maximizing the controls for security and privacy of collected data;

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction and does not include mere transit of data originating outside Nigeria;

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing;

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"Sensitive Personal Data" means personal data relating to an individual's (a) genetic and biometric data, for the purpose of uniquely identifying a natural person; (b) race or ethnic origin; (c) religious or similar beliefs, such as those reflecting conscience of philosophy; (d) health status; (e) sex life; (f) political opinions or affiliations; (g) trade union memberships; (h) other information prescribed by the NDPC as sensitive personal data;

"Third Party" means any natural or legal person, public authority, establishment or any other body other than the Data Subject, the Data Controller, and the persons who are engaged by the Data Controller to process Personal Data.

2. INTRODUCTION

2.1 In the growing digital economy, responsible, ethical and lawful data processing forms the foundation of digital trust in any organisation processing Personal Data of Data Subjects. Branch International Finance Company Limited ("Branch" or the "Company") collects, uses, stores, and otherwise processes Personal Data relating to a variety of stakeholders, including employees (current and former), applicants, customers (current and former), contractors, workers, interns, website and application users, and other contacts, collectively referred to in this Policy as Data Subjects.

2.2 Branch is committed to ensuring the responsible and lawful processing of Personal Data in accordance with applicable Data Protection Laws. This Policy outlines the principles, standards, and responsibilities undertaken by Branch to ensure compliance with these laws and to protect the rights of individuals whose data we process.

2.3 This Policy shall be read in conjunction with the Privacy Policy, the Data Deletion and Retention Standard Operating Procedure, and other related policies and procedures.

3. PURPOSE

This Policy seeks to ensure that Branch:

a. is clear about how Personal Data must be processed and its expectations for those who process Personal Data on its behalf;

b. complies with the Data Protection Laws and with good practice;

c. protects its reputation by ensuring the Personal Data entrusted to it is processed in accordance with the principles of data protection and in recognition of Data Subjects' rights; and

d. protects itself from risks of Personal Data Breaches and other breaches of the Data Protection Laws.

4. SCOPE

4.1 This Policy applies to;

a. all employees, management, board, contractors, service providers, and other third parties who process Personal Data on behalf of Branch; and

b. all Personal Data processed by or on behalf of Branch, regardless of the medium or location of the data.

4.2 Every employee of Branch is required to read and assimilate the contents of this Policy and to abide by it fully. Branch shall have the right to seek redress against any employee whose failure to comply with this Policy in any manner whatsoever results in damages being sought or awarded, or any legal action instituted against Branch.

4.3 The DPO is responsible for overseeing this Policy. Branch's DPO can be reached at ngdpo@branch.co

5. PERSONAL DATA PROTECTION PRINCIPLES

5.1 In adherence to the Data Protection principles, Branch shall ensure that Personal Data is:

i. processed lawfully, fairly, and in a transparent manner, with due regard for the dignity and rights of the Data Subject.

ii. collected for specified, explicit, and legitimate purposes, and shall not be further processed in any manner that is incompatible with those purposes.

iii. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is collected and processed.

iv. accurate, complete, not misleading, and, where necessary, kept up to date, having regard to the purpose for which the personal data is collected or is further processed.

v. stored only for as long as is necessary for the purposes for which the Personal Data is processed, and no longer.

vi. processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, and against accidental loss, destruction, or damage, using suitable technical and organizational measures.

vii. processed in accordance with the data protection principles, and shall take full responsibility for, and be able to demonstrate, compliance with these principles.

6. CONSENT

6.1 Branch shall obtain a Data Subject's Consent if there is no other Lawful Basis for the Processing. Consent requires genuine choice and genuine control.

6.2 A Data Subject Consents to the Processing of his or her Personal Data if he or she clearly indicates agreement either by a statement or positive action to the Processing. Consent must be specifically and expressly given. If Consent is given in a document that deals with other matters, Branch must ensure that the Consent is separate and distinct from those other matters.

6.3 Prior to giving Consent, the Data Subject shall be informed of his or her right and the ease to withdraw his or her Consent at any time. Withdrawal of Consent must be promptly honoured once the Data Subject withdraws it.

6.4 Consent might need to be renewed if Branch intends to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented, or if the Consent is historic.

6.5 Branch shall store event tracking information that serves as evidence of the Consent to demonstrate compliance to consent.

6.6 No Consent shall be sought, given or accepted in any circumstance that may engender direct or indirect propagation of atrocities, hate, child rights violations, criminal acts and anti-social conduct.

7. DATA COLLECTION

7.1 Branch collects the following information: name, data of birth, telephone number, email address, nationality, tax identity number, bank details, bank verification number, an identity number, address, selfie, occupation, industry, employer/company name, source of funds, and other relevant information which constitute Personal Data.

7.2 When Data Subjects send email or other communications to Branch, such communications may be retained in order to process inquiries, respond to their requests and improve Branch services.

7.3 Branch collects the above-mentioned information for evaluation during onboarding, for due diligence, and regulatory compliance, among other reasons.

7.4 Prior to collecting Personal Data from the Data Subject, Branch shall provide the Data Subject with all of the following information:

a. identity and contact details of Branch;

b. the email address of the DPO;

c. the purpose of the Processing for which the Personal Data is intended, as well as the lawful basis for the Processing;

d. the legitimate interests pursued by Branch or by any Third Party who has access to the Personal Data;

e. the recipients or categories of recipients of the Personal Data (if any);

f. where applicable, the fact that Branch intends to transfer Personal Data to a recipient in a foreign country or a third country or international organisation and the existence or absence of an adequacy of protection ;

g. the existence of the right to withdraw Consent for continuous data processing at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal;

h. the retention period of the personal data;

i. the right to lodge a complaint with NDPC or any other relevant authority;

j. whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;

k. where Branch intends to further process the Personal Data for a purpose other than that for which the Personal Data is collected, Branch shall provide the Data Subject prior to the further Processing, with information on that other purpose and with any relevant information.

7.5 Personal data must be accurate, and kept up to date.

7.6 Branch should ensure that Personal Data is recorded in the correct files.

7.7 Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, Branch should ensure that relevant records are completed.

8. LAWFUL BASIS FOR DATA PROCESSING

8.1 Branch must ascertain that the processing of the data is lawful.

8.2 Processing shall be lawful if at least one of the following applies:

a. the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes;

b. Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

c. Processing is necessary for compliance with a legal obligation to which the Controller is subject;

d. Processing is necessary in order to protect the vital interests of the Data Subject or another person;

e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller; and

f. Processing is necessary for the purposes of the legitimate interest pursued by Branch or by the third party to whom the data is disclosed provided it does not breach the fundamental rights of the Data Subjects.

9. DATA SUBJECT RIGHTS

Data subjects have rights in relation to the way Branch handles their Personal Data. These rights include :

a. where the Lawful Basis of our Processing is Consent, the right to withdraw that Consent to process their personal data;

b. the right to know the purposes of processing and the categories of personal data concerned;

c. the right to know the recipients or categories of recipient to whom the personal data have been or will be disclosed, particularly recipients in third countries or international organizations;

d. where possible, the right to know the period for which personal data will be stored, or if not possible, the criteria used to determine that period;
e. the right to ask Branch to rectify inaccurate data or to complete incomplete data or restrict Processing in specific circumstances e.g. where there is a valid complaint about accuracy;

f. the right to request from Branch, the erasure of personal data;

g. the right to request and obtain access to their Personal Data held by Branch. This includes the right to know whether their Personal Data is being processed and to receive a copy of the data. Provided that where providing such data would impose unreasonable costs on Branch, the data subject may be required to bear some or all of such costs;

h. the right to request their Personal Data in a structured, commonly used, and machine-readable format and have it transferred to another data controller where technically feasible;

i. the right not to be subject to decisions based solely on automated Processing, including Profiling, except where necessary for entering into, or performing, a contract, with Branch; it is based on the Data Subject's explicit Consent; or is authorised by law and is also subject to safeguards;

j. the right to prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k. the right to be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and

l. the right to make a complaint to NDPC or any other regulatory body.

10. DATA SUBJECT REQUESTS

10.1 Branch shall take appropriate measures to provide any information relating to Personal Data Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular, for any information addressed specifically to a Data Subject.

10.2 The information may be provided by electronic means.

10.3 Branch shall verify the identity of the Data Subject requesting data. Where there is reasonable doubt concerning the identity of the person making the request for

information, Branch may request the provision of additional information necessary to confirm the identity of the Data Subject.

10.4 Branch shall immediately forward any Data Subject Access Request received to the Data Protection Officer at ngdpo@branch.co.

10.5 Information provided to the Data Subject and any communication and any action taken shall be provided free of charge. Where the Data Subject's request is manifestly unfounded or excessive, in particular because of their repetitive character, Branch may either:

a. charge a reasonable fee taking into account the administrative costs of providing the information or communicating or taking the action requested; or

b. write a letter to the Data Subject stating refusal to act on the request and copy NDPC on every such occasion.

10.6 Branch shall not allow third parties to persuade it into disclosing Personal Data without proper authorisation. For example, employee spouses do not have an automatic right to gain access to their spouse's data.

10.7 Branch shall make best efforts to not alter, conceal, block or destroy Personal Data once a request for access has been made.

11. ACCOUNTABILITY

11.1 Branch shall implement appropriate technical and organisational measures in an effective manner to ensure compliance with the personal data protection principles. Branch is responsible for, and must be able to demonstrate compliance with, the Personal Data protection principles in Paragraph 5 above.

11.2 Branch shall apply adequate resources and controls to ensure and to document the Data Protection Laws compliance including:

a. appointing a suitably qualified DPO and actively involving the DPO in all personal data processing matters, providing necessary resources, access, and continuous training, ensuring independence without coercion or penalty, and enabling direct reporting to management level;

b. Integrating data protection into Branch's policies and procedures, in the manner Personal Data is handled by Branch, and by producing required documentation such as privacy notices, records of processing activities, and records of Personal Data Breaches;

c. training members of staff on compliance with Data Protection Laws and keeping a record accordingly; and

d. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

11.3 Branch shall engage the services of a Data Protection Compliance Organization and file its Annual Compliance Audit Report on or before the 31st of March each year.

12. DATA SECURITY

12.1 Branch shall implement and sustain appropriate safeguards to protect Personal Data, taking into account in particular the risks to Data Subjects presented by unauthorised or unlawful Processing or accidental loss, destruction of, or damage to their Personal Data.

12.2 Safeguarding will include the use of encryption and Pseudonymisation where appropriate. It also includes protecting confidentiality (i.e. that only those who need to know and are authorised to use Personal Data have access to it), integrity and availability of the Personal Data. We will regularly evaluate and test the effectiveness of those safeguards to ensure the security of our Processing of Personal Data.

12.3 Branch shall also implement measures for protecting the Personal Data that it processes in the course of its duties. Branch shall handle Personal Data in a way that guards against accidental loss or disclosure or other unintended or unlawful Processing and in a way that maintains its confidentiality. Branch shall exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

12.4 Branch shall take steps to comply with procedures and technologies put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

12.5 Branch shall take steps to comply with all applicable aspects of this Policy, and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained in accordance with the Data Protection Laws standards to protect Personal Data

13. ROLES AND RESPONSIBILITIES

In compliance with the Data Protection Laws, Branch has identified key stakeholders and their responsibilities to drive the operationalisation of this Policy and implementation of necessary data protection controls.

13.1 Board

The Board is responsible for:

a. setting the tone at the top on data protection
b. ensuring that Branch meets the obligations of the Data Protection Laws.

13.2 Management

The Senior Management is responsible for:

a. ensuring data protection objectives are established and are aligned with the strategic direction of the Company
b. providing necessary resources to the DPO to carry out data protection tasks;
c. making adequate provision for continuous training for the DPO.

13.3 Data Protection Officer

13.3.1 The DPO is responsible for:

a. advising Branch and its employees of its obligations under the Data Protection Laws;

b. monitoring compliance with this Policy and Data Protection Laws,

c. providing advice where requested on Data Protection Impact Assessments;

d. supervising internal data processing;

e. dealing with requests, complaints and enquiries from Data Subjects and law enforcement agencies;

f. cooperating with and acting as the contact point between Branch and Data Subject or NDPC;

g. carrying out regular routine checks on Data Protection compliance practices without notice to employees;

h. preparing and keeping Semi-Annual Data Protection Reports (SAPR) as provided for under the Data Protection Laws.

13.3.2 The DPO shall in the performance of his or her tasks have due regard to the risk associated with Processing operations, taking into account the nature, scope, context and purposes of Processing.

13.3.3 The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with relevant legislation.

13.3.4 Branch shall give appropriate support to the DPO in performing the data protection responsibilities.

13.3.5 The DPO shall directly report to the management of Branch.

13.4 Employees

13.4.1 Employees who process Personal Data of Branch employees, Board, customers, clients, applicants, or any other individual must comply with the requirements of this Policy. Employees must ensure that:

a. all Personal Data is kept securely;
b. no Personal Data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised Third Party;
c. Personal Data is kept in accordance with this Policy;
d. any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO;
e. any data protection breaches are swiftly brought to the attention of the DPO and that they support the DPO in resolving breaches; and
f. where there is uncertainty around a data protection matter, advice is sought from the DPO before taking any action.

13.4.2 Where employees responsible for ad hoc staff or short-term staff or volunteers or contractors or interns or any person by whatever name called, undertake responsibilities which involve the Processing of personal data, they must ensure that such person is aware of the data protection principles and obligations detailed in this Policy.

13.4.3 Employees who are unsure about who are the authorised Third Parties to whom they can legitimately disclose Personal Data should seek advice from the DPO.

13.4.4 Branch employees may only process Personal Data when required for the performance of their job duties and shall not process Personal Data for any purpose unrelated to their official responsibilities.

14. THIRD-PARTY DATA PROCESSORS

14.1 Data Processing by a Third Party shall be governed by a written contract between the Third Party and Branch.

14.2 Where a Third-Party data processor is used:

a. the Third-Party data processor shall be chosen by Branch and the data processor must provide sufficient guarantees about its organizational and technical measures to protect the Processing of Personal Data;

b. reasonable steps must be taken by the DPO to ensure that such technical and organizational measures are in place;

c. a written contract establishing what Personal Data will be processed and for what purpose, provided by the Compliance team, must be entered into by both parties i.e. the Third-Party Data Processor and Branch.

14.3 Branch shall ensure that the Third-Party Data Processor does not have a record of violating the principles of data Processing and that the Third Party is accountable to NDPC or a reputable regulatory authority for data protection within or outside Nigeria.

14.4 Branch may only transfer Personal Data to Third Party service providers (i.e. Data Processors) approved by the DPO who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Laws and who agree to act only on Branch's instructions.

14.5 For further guidance about the use of Third-Party Data Processors please contact the DPO or Data Protection team.

15. CONTRACTORS, SHORT-TERM AND VOLUNTARY STAFF

15.1 Branch is responsible for the use of Personal Data by anyone working on its behalf. Managers who employ contractors or short term or voluntary staff must ensure that they are appropriately vetted for the data they will be Processing. In addition, managers should ensure that:

a. any Personal Data collected or processed in the course of work undertaken for Branch is kept securely and confidentially;

b. all Personal Data is returned to Branch on completion of the work, including any copies that may have been made. Alternatively, the data is securely destroyed

and Branch receives notification in this regard from the contractor or short term / voluntary member of staff;

c. Branch shall receive prior notification of any disclosure of Personal Data to any other organisation or any person who is not a direct employee of the contractor;

d. any Personal Data made available by Branch, or collected in the course of the work, is neither stored nor processed outside Nigeria unless written Consent to do so has been received from Branch; and

e. all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any Personal Data beyond what is essential for the work to be carried out properly.

15.2 For further guidance on this item, please contact the DPO or Data Protection team.

16. REPORTING A PERSONAL DATA BREACH

16.1 Branch is required to report to the Commission any Personal Data Breach which is likely to result in a risk to the rights and freedoms of the Data Subject. Where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the Personal Data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the Data Subject directly. In the latter circumstances, a public communication must be made, or an equally effective alternative measure must be adopted to inform Data Subjects, so that they themselves can take any remedial action.

16.2 Branch shall put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the relevant regulator where it is legally required to do so.

16.3 Branch shall, within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals, notify the NDPC of the breach and furnish them with all relevant information. Branch shall take all reasonable measures to promptly remedy any breach or suspected breach of Personal Data.

16.4 Any employee or member of staff who knows or suspects that a Personal Data Breach has occurred, should immediately contact the Data Protection team at ngdpo@Branch.co Branch will retain all evidence relating to Personal Data Breaches in particular to enable Branch to maintain a record of such breaches, as required by the Data Protection Laws.

16.5 Records of Personal Data Breaches must be kept by each employee or member of staff who observes or has reason to believe that a Data Breach has occurred. The record must set out:

a. the facts surrounding the breach;
b. its effects; and
c. the remedial action taken.

16.6 Branch will not be responsible for any Personal Data breach which occurs as a result of:

a. an event which is beyond the reasonable control of Branch;

b. an act or threats of terrorism;

c. an act of God (such as, but not limited to fires, explosions, earthquakes, drought, tidal waves and floods) which compromises Branch's data protection measures;

d. war, hostilities (whether war be declared or not), invasion, act of foreign enemies, mobilisation, requisition, or embargo; and

e. rebellion, revolution, insurrection, or military or usurped power, or civil war which compromises Branch's data protection measures;

f. the transfer of Data Subject's Personal Data to a third party on their instructions; and

g. the use of Data Subject's personal data by a third party designated by them.

17. LIMITATIONS ON THE TRANSFER OF PERSONAL DATA

17.1 Where it is intended that Personal Data shall be transferred to a foreign country or an international organisation for processing, such transfer shall only occur if the recipient ensures an adequate level of data protection in accordance with the NDPA. The adequacy of protection shall be determined based on the criteria set out in Section 42 of the NDPA. Adequacy of protection is assessed based on factors such as enforceable Data Subject rights, the existence of a data protection law, regulatory oversight, international commitments, and so on.

17.2 Where an adequate level of protection is not established, Personal Data may only be transferred outside Nigeria under specific conditions, including:

a. the Data Subject has explicitly Consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards and that there are no alternatives;

b. the transfer is necessary for the performance of a contract between the Data Subject and Branch or the implementation of pre-contractual measures taken at the Data Subject's request;

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between Branch and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;

e. the transfer is necessary for the establishment, exercise or defence of legal claims; and

f. the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving Consent.

17.4 Where personal data is transferred outside Nigeria, Branch shall ensure that:

a. The recipient organization has implemented adequate safeguards, such as a data protection agreement or cross-border transfer instrument that meets NDPA requirements;
b. The Data Subjects' rights are protected in the receiving country;
c. Data subjects are informed about the cross-border transfer and the measures in place to protect their personal data.

17.5 Before transferring personal data to a third party (within or outside Nigeria), Branch shall enter into a Data Processing Agreement with the recipient or include specific data transfer clauses in the relevant contract entered with such third party. The agreement shall include:

a. Obligations requiring the receiving party to comply with Nigerian data protection laws;
b. Security measures to be implemented to protect the personal data;
c. Restrictions on further transfers without prior authorization;
d. Mechanisms for monitoring compliance, including audits and reporting requirements;
e. Rights of Data Subjects and mechanisms for enforcing those rights.

17.6 In cases where no adequate level of protection exists in the receiving country, additional safeguards, such as encryption, anonymization, or pseudonymization, may be required before the transfer is executed.

18. TRAINING AND AUDIT

18.1 Branch is required to develop and implement a privacy training schedule; circulate internal privacy checklists and ensure that all its employees undergo adequate training to enable them to comply with Data Protection Laws.

18.2 Branch shall regularly test its systems and processes to assess compliance with data protection laws.

18.3 Branch shall have a written schedule for the general review of all of its data processing platforms and practices, and check for data protection compliance when procuring new software or features that require Data Processing.

18.4 Branch shall conduct an Annual and Semi-Annual Data Protection Assessment in line with the provisions of the Data Protection Laws.

19. SHARING PERSONAL DATA

19.1 In the absence of Consent, a legal obligation or other legal basis of Processing, Personal Data should not generally be disclosed to Third Parties unrelated to Branch, with the exception of Third Parties service providers like - Payroll Managers, Pension Funds Administrators, as well as disclosures to regulatory authorities and credit bureaus. In cases of loan default, relevant Personal Data may also be shared with collections agencies, strictly in accordance with applicable laws and contractual obligations.

19.2 Further, without a court order, the law enforcement agencies and their agents have no automatic right of access to records of Personal Data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. Law Enforcement Agents that request Personal Data should be referred to the DPO.

19.3 Sharing of Personal Data for research purposes may also be permissible, subject to certain safeguards. If you need guidance or clarification, please contact the Data Protection team on [ngdpo@Branch.co]

20. DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

Branch shall conduct a Data Protection Impact Assessment (DPIA) for any processing activity that is likely to result in a high risk to the rights and freedoms of Data Subjects, in accordance with the NDPA. The DPIA shall be carried out before initiating such Processing and shall include the following steps:

a. Branch shall assess the processing activity by identifying and documenting the nature, scope, context, and purpose of the processing. This assessment shall determine whether the processing involves special categories of data, large-scale processing, automated decision-making, or profiling.

b. Identify and evaluate potential risks associated with the processing. This includes assessing the possible impact on Data Subjects, such as risks to privacy, security, and fundamental rights, and identifying potential threats, including data breaches, unauthorised access, or misuse of personal data.

c. Branch shall evaluate whether the processing is essential to achieve its intended purpose and ensure that it aligns with data protection principles such as data minimization, purpose limitation, and security safeguards.

d. To mitigate identified risks, Branch shall implement appropriate technical and organizational measures. These may include encryption, pseudonymization, access controls, and the establishment of data retention policies to enhance security and compliance.

e. All findings, decisions, and risk mitigation strategies shall be documented, and a detailed record of the DPIA shall be maintained. Where the DPIA indicates that the processing of the data would result in a high risk to the rights and freedoms of Data Subjects, Branch shall submit the DPIA to the Nigeria Data Protection Commission (NDPC) for review.

f. The DPIA shall contain measures which guarantee privacy by design and default.

g. The DPIA shall be subject to periodic review and monitoring, particularly when there are changes in processing activities or regulatory requirements. Any necessary updates to risk mitigation measures shall be implemented to maintain compliance with data protection laws.

The DPO shall oversee the entire DPIA process, ensuring that high-risk processing activities are conducted in full compliance with the NDPA.

21. POLICY REVIEW

This Policy shall be reviewed every three (3) years, or sooner if required, whichever occurs first. The review process will take into account any changes or updates to Data Protection Laws industry best practices and standards relevant to Branch. Following the review, the Policy, along with any amendments, shall be submitted to the Board for approval.

APPROVED BY THE BOARD OF DIRECTORS

THIS 19TH DAY OF MAY 2025

CHAIRMAN	**COMPANY SECRETARY**