DATA PROTECTION POLICY NIGERIA	
APPROVING AUTHORITY	General Manager, Nigeria
SIGNATURE	
APPROVAL DATE	25th April, 2019
REVIEW DATE	24th April, 2019

1. DEFINITIONS

"Automated Decision-Making" means when a decision is made which is based solely on automated Processing (including Profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated Processing;

"Consent" means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her;

"Data Controller" means a person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed;

"Data Subject" means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

"Data Protection Impact Assessment or DPIA" means tools and assessments used to identify and reduce risks of a data Processing activity. DPIA can be carried out

as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data;

"Data Protection Laws" means the NDPR, the GDPR and any relevant data protection laws;

"Data Protection Officer or 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, for monitoring compliance with Data Protection Laws, as well as with Branch's policies and providing advice;

"GDPR" means the EU General Data Protection Rules 2016/679;

"Legal Basis" means the basis for Processing Personal Data as set out in Paragraph 7 of this Policy

"NDPR" means Nigeria Data Protection Regulation 2019;

"NITDA" means National Information Technology Development Agency;

"Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others;

"Personal Data Breach" means a breach of security leading 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 GDPR;

"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 or alteration, retrieval, consultation, use, disclosure by transmission, dissemination

or otherwise making available, alignment or combination, restriction, erasure or destruction;

"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 replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure;

"Sensitive Personal Data" means Data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views trade union membership, criminal records or any other sensitive personal information;

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

"Branch" means Branch International Inc.

2. INTRODUCTION

2.1 Branch takes its responsibilities with regard to the management of the requirements of the Data Protection Laws very seriously. This Policy sets out how Branch manages these responsibilities.

2.2 Branch obtains, uses, stores and otherwise processes Personal Data relating to potential users, employees (applicants) and clients, current employees and clients, former employees and clients, current and former workers, contractors, website and application users and contacts, collectively referred to in this Policy as Data Subjects. When Processing Personal Data, Branch is obliged to fulfill individuals' reasonable expectations of privacy by complying with the Data Protection Laws.

2.3 This Policy therefore seeks to ensure that Branch:

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

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

c. protect its reputation by ensuring the Personal Data entrusted to us is processed in accordance with Data Subjects' rights; and

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

3. SCOPE

3.1 This Policy applies to all Personal Data we process regardless of the location where that Personal Data is stored (e.g. on a user's own device) and regardless of the Data Subject. All users and others Processing Personal Data on Branch's behalf must read it. A failure to comply with this Policy may result in disciplinary action.

3.2 Every member of staff 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 member of staff 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.

3.3 The Data Protection Officer is responsible for ensuring that all Branch employees comply with this Policy and should implement appropriate practices, processes, controls and training to ensure compliance.

3.4 The DPO is responsible for overseeing this Policy. Branch's DPO is the Head of Engineering, and he can be reached at [dpo]@branch.co

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 When we process Personal Data, we are guided by the following principles, which are set out in the Data Protection Laws. Branch is responsible for, and demonstrates compliance with the data protection principles listed below:

4.2 Those principles require Personal Data to be:

1. processed lawfully, fairly, in a transparent manner and with respect for the dignity of the human person.

2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

4. accurate and where necessary kept up to date.

5. not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Personal Data is processed.

6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

5. CONSENT

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

5.2 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, you must ensure that the Consent is separate and distinct from those other matters.

5.3 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 by uninstalling the app. Withdrawal of Consent must be promptly honoured once the data subject uninstalls the app.

5.4 Consent might need to be renewed if we intend 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.

5.5 Branch will store event tracking information that serve as evidence of the Consent to demonstrate compliance to consent.

5.6 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.

6. DATA COLLECTION

6.1 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, location, photograph, IP address, MAC address, IMEI number, IMSI number and other information relevant which constitute Personal Data.

6.2 Branch collects the above-mentioned information using in-app forms and through information gathered from the device.

6.3 When users send email or other communications to Branch, we may retain those communications in order to process inquiries, respond to their requests and improve our services. When clients access Branch's services, the Branch servers automatically record information that the customer's/client's browser sends whenever a person visits a website.

6.4 Branch collects the above-mentioned information for evaluation of credit risk, due diligence, regulatory compliance, and marketing among other reasons.

6.5 Prior to collecting Personal Data from the Data Subject, Branch shall provide the Data Subject with all of the following information contained in the privacy and security policy

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 legal 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 and the existence or absence of an adequacy decision by NITDA;

g. concerning the Data Subject or to object to Processing as well as the right to data portability;

h. the existence of the right to withdraw Consent for continuous data access at any time by uninstalling the app, without affecting the lawfulness of Processing based on Consent before its withdrawal;

i. the right to lodge a complaint with NITDA 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.

6.7 Personal data must be accurate and, where necessary, kept up to date.

6.8 You should ensure that Personal Data is recorded in the correct files.

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

7. DATA PROCESSING

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

7.2 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 of another natural person; and

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.

8. DATA SUBJECTS' RIGHTS

Data subjects have rights in relation to the way we handle their Personal Data. These include the following rights:

1. where the Legal Basis of our Processing is Consent, to withdraw that Consent to process additional information by uninstalling the app

2. to object to our Processing of Personal Data in limited circumstances; and

3. to ask us to rectify inaccurate data or to complete incomplete data;

4. to restrict Processing in specific circumstances e.g. where there is a valid complaint about accuracy;

5. 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;

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

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

8. to make a complaint to NITDA or any other regulatory body; and

9. REQUESTS

9.1 Branch shall take appropriate measures to provide any information relating to 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 child.

9.2 The information may be provided by electronic means.

9.3 We verify the identity of an individual requesting data. Where you have reasonable doubt concerning the identity of the person making the request for information, you may request the provision of additional information necessary to confirm the identity of the Data Subject.

9.4 We immediately forward any Data Subject Access Request you receive to the Data Protection Officer at dpo@branch.co.

9.7 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 NITDA on every such occasion.

9.8 We do not allow third parties to persuade you into disclosing Personal Data without proper authorisation. For example, customers'/clients' spouses do not have an automatic right to gain access to their spouse's data. Parents of Data Subjects do not have an automatic right to gain access to their child's data.

9.9 We should not alter, conceal, block or destroy Personal Data once a request for access has been made. You should contact dpo@branch.co before any changes are made to Personal Data which is the subject of an access request.

10 ACCOUNTABILITY

10.1 We 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 above.

10.2 We apply adequate resources and controls to ensure and to document the Data Protection Laws compliance including:

10.2.1 appointing a suitably qualified DPO;

10.2.2 integrating data protection into our policies and procedures, in the way Personal Data is handled by us and by producing required documentation such as privacy notices, records of Processing and records of Personal Data Breaches;

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

10.2.4 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 DATA SECURITY

11.1 Branch implements and sustains 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.

11.2 Safeguarding will include the use of encryption and Pseudonymisation where appropriate. It also includes protecting the 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.

11.3 Branch also implements measures for protecting the Personal Data that you process in the course of your duties. We 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. We also exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

11.4 We take steps to comply with procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

11.5 We take steps to comply with all applicable aspects of this Policy, and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Laws standards to protect Personal Data.

12 RESPONSIBILITIES OF THE DPO

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. Branch's policies with respect to data protection and monitoring, training and audit activities that relate to compliance with the Data Protection Laws;

d. providing advice where requested on data protection impact assessments;

e. supervising internal data processing;

f. dealing with requests, complaints and enquiries from Data Subject and law enforcement agencies;

g. to cooperate with and act as the contact point between Branch and NITDA; and

h. the data protection officer 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 EMPLOYEE RESPONSIBILITIES

13.1 Employees who process Personal Data about Branch employees, clients, applicants, alumni 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 and the [Data Protection team;

e. any data protection breaches are swiftly brought to the attention of the Data Protection team and the DPO and that they support the Data Protection team in resolving breaches; and

f. where there is uncertainty around a data protection matter advice is sought from the Data Protection team and the DPO.

13.2 Where employees are responsible for adhoc staff or short-term staff or volunteers or contractors or interns or any person by whatever name called, doing work which involves the Processing of personal information, they must ensure that such person is aware of the data protection principles.

13.3 Employees who are unsure about who are the authorised third parties to whom they can legitimately Disclose Personal Data should seek advice from the Data Protection team or the DPO.

13.4 Branch employees may only process Personal Data when performing job duties requires it and should not process Personal Data for any reason unrelated to job duties.

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 external companies are used to process Personal Data on behalf of Branch, responsibility for the security and appropriate use of that data as long as it remains with Branch.

14.3 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 security measures to protect the Processing of Personal Data;

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

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

14.4 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 NITDA or a reputable regulatory authority for data protection within or outside Nigeria.

8.5 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.

14.6 For further guidance about the use of Third-Party data processors please contact Data Protection team.

15. CONTRACTORS, SHORT-TERM AND VOLUNTARY STAFF

15.1 Branch is responsible for the use made 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 receives 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.

16 CUSTOMER/CLIENT AND USER RESPONSIBILITIES

Customers/Clients and Users are responsible for:

a. familiarising themselves with the privacy policy provided when their relationship with Branch commences;

b. ensuring that their Personal Data provided to Branch is accurate and up to date.

17 REPORTING A PERSONAL DATA BREACH

17.1 Branch required to report any Personal Data Breach where there is a risk to the rights and freedoms of the Data Subject. Where the Personal Data Breach results in a high risk to 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.

17.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or the relevant regulator where we are legally required to do so. All suspected breach of Personal Data should be remedied with 1 (one) month from the date of the report of the breach.

17.3 If you know or suspect that a Personal Data Breach has occurred, you should immediately contact the Data Protection team at dpo@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.

17.4 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.

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

a. an event which is beyond the 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 your personal data to a third party on your instructions; and

g. the use of your personal data by a third party designated by you.

18 LIMITATIONS ON THE TRANSFER OF PERSONAL DATA

18.1 where it is intended that Personal Data shall be transferred to a foreign country or to an international organisation for processing, the affirmation of the Attorney-General of the Federation, that the data protection levels in the foreign country or international organisation are adequate in accordance with the provisions of the NITDA regulations, must be obtained.

18.2 An application to the Attorney General of the Federation shall be accompanied by all data protection laws applicable to the foreign data processor, including all data protection policies of the said foreign recipient.

18.3 In the absence of any decision by the Attorney-General of the Federation as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of Personal Data to a foreign country or an international organisation shall take place only on one of the following conditions:

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.

18.4 Provided, in all circumstances above, that the Data Subject shall be manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, except where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

19 20 TRAINING AND AUDIT

20.1 We are required to ensure that all Branch employees undergo adequate training to enable them to comply with Data Protection Laws. We also periodically regularly test our systems and processes to assess compliance.

20.2 We carry out data privacy related training.

20.3 We periodically review systems and processes under our control to ensure they comply with this Policy.

22. DIRECT MARKETING

22.1 We are subject to certain rules and privacy laws when marketing to our customers/clients and potential customers/clients, alumni and any other potential user of our services. The limited exception for existing customers/clients allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person they are marketing similar services.

23 SHARING PERSONAL DATA

23.1 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 reports to credit bureaus and contact information that is shared with collections agencies should the user fail to pay their loan.

23.2 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. You should refer law enforcement agents that request Personal Data to the DPO.

23.3 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 [do@Branch.co].

24. CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time without notice to you. We will, however, notify you any time this Policy is amended.