DATA PROCESSING ANNEX

PREAMBLE:

A. Interswitch and the User have entered into the Agreement which may result in a Party (“Controller”) transferring a Data Subject’s Personal Data to the other Party (“Processor”) to enable the effective performance of the Service, the effective performance of an underlying obligation between the Data Subject and the Controller or Processor or for any other purpose permitted under the Data Protection Laws.

B. This Data Processing Annex complements the Agreement and shall not amend any aspect of the Service, besides the handling and processing of the Data Subject’s Personal Data.

C. The Parties agree to the terms of this Data Processing Annex to ensure the protection and security of any Personal Data transferred from either party acting as Controller to the other party acting as Processor, in accordance with the Data Protection Laws.

1. DEFINITIONS AND INTERPRETATION

"**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity;

“**Business Days**" means a day other than a Saturday, Sunday or public holiday on which banks are open for general business in Lagos, Nigeria;

"**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" shall be construed accordingly;

“**Data**” means the quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media;

"**Data Protection Laws**" means all data protection laws and regulations applicable to a Party's processing of Personal Data under the Agreement, including the Nigeria Data Protection Regulation, 2019 or any modification or amendment thereof;

“**Data Subject**” means a natural person who can be identified directly or indirectly by reference to the Personal Data collected by the Parties;

“**PCI Standards**” means the information security standards administered by the Payment Card Industry Security Standards Council;

"**Personal Data**" means any information relating to a Data Subject and containing an identifier such as a name, an identification number, location data, photo, email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to Media Access Control (MAC) address, Internet Protocol (IP) address, International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, Subscriber Identification Module (SIM). Personal Data shall include any online identifier or any one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that Data Subject;

“**Processing and Process**" either mean any activity that involves the use of Personal Data or as the Data Protection Laws may otherwise define processing or process. It includes any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organising, structuring, storing, adapting or altering, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, Processing also includes transferring Personal Data to third parties;

"**Security Incident**" means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, or alteration of, or unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise processed;

“**Security Measures**” means processes adopted by each Party to protect its Data. Such measures include but not limited to protecting systems from hackers, cyberattacks, viral attack, data theft, damage by rain, fire or exposure to other natural elements. These measures also include setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of email systems and continuous capacity building for staff;

"**Sensitive Data**" means (a) passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the masked (last four digits) of a credit or debit card); (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" under applicable Data Protection Laws; and

"**Sub-processor**" means any processor engaged by a Processor or its Affiliates to assist in fulfilling its obligations with respect to providing the Service according to the Agreement or this Data Processing Annex. Sub-processors may include third parties or Affiliates of the Processor but shall exclude the Processor’s employees or consultants.

2. ROLES AND RESPONSIBILITIES

THE PARTIES

2.1 Each Party shall implement and maintain effective Security Measures that are designed to preserve the security and confidentiality of each Party’s Data and protect its Data from Security Incidents. For Personal Data, such effective Security Measures include pseudonymisation and encryption of Personal Data.

2.2 Each Party shall ensure it implements a process for regularly testing, assessing and evaluating the effectiveness of its Security Measures.

CONTROLLER

2.3 Controller will not provide (or cause to be provided) any Sensitive Data to Processor for processing under the Agreement without the express consent of the Data Subject. The

Parties understand that Sensitive Data merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms of the Data Subject.

2.4 Controller represents and warrants that

2.4.1 it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its processing of Personal Data and any processing instructions it issues to Processor; and

2.4.2 it has obtained and will continue to obtain, all consents and rights necessary under Data Protection Laws for Processor to process Personal Data for the purposes described in the Agreement.

2.5 Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data.

2.6 Controller will ensure that Processor's processing of the Controller's Data following Controller's instructions will not cause Processor to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws.

THE PROCESSOR

2.7 Processor shall adopt such measures to ensure a level of security appropriate to the sensitivity of the Data transferred to the Processor. These measures include the pseudonymisation and encryption of personal data.

2.8 Processor shall notify Controller in writing within 48 (forty-eight) hours, unless prohibited from doing so under Data Protection Laws, if it becomes aware or believes that any data processing instruction from Controller violates any Data Protection Law.

2.9 Processor shall ensure it can restore the availability and access to Personal Data promptly in the event of a Security Incident.

2.10 Processor shall ensure that any person who is authorised by Processor to process Personal Data (including its staff, agents and subcontractors) shall be under a contractual or statutory obligation of confidentiality.

2.11 Processor shall in updating or modifying its Security Measures, ensure that such updates and modifications do not result in the degradation of the Processor's Security Measures.

2.12 Upon becoming aware of a Security Incident, Processor shall:

2.12.1 notify Controller without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Incident;
2.12.2 provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Controller; and
2.12.3 promptly take reasonable steps to contain and investigate any Security Incident.

2.13 Processor's notification of or response to a Security Incident under clause 2.12 shall not be construed as an acknowledgement by Processor of any fault or liability concerning the Security Incident.

2.14 Notwithstanding the above, Controller agrees that except as provided in this Agreement, Controller is responsible for protecting the security of Personal Data when in transit to the Processor while the Processor is responsible for protecting the security of Personal Data it receives and transfers to any party including any Sub-Processor.

3. SUB-PROCESSING

3.1 Controller agrees that the Processor may engage Sub-processors to process Personal Data on Controller's behalf.

3.2 Processor shall notify Controller of any engagement or disengagement of a Sub-processor.

3.3 Processor shall:

3.3.1 enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Controller’s Data as those in this Agreement; and

3.3.2 remain responsible for the Sub-processor’s compliance with the obligations of this Data Processing Annex and for the acts or omissions of such Sub-processor that cause Processor to breach any of its obligations under this Data Processing Annex.

4. SECURITY REPORTS AND AUDITS

Clauses 4.1 and 4.2 shall apply to Processors that are annually audited against PCI Standards and clauses 4.3 and 4.4 shall apply to Processors that are not annually audited against PCI Standards.

4.1 Processor shall supply (on a confidential basis) a copy of its annual attestation of compliance and certificate of compliance ("Reports") to Controller within five (5) Business Days of Controller’s written request, to enable Controller verify Processor's compliance with the audit standards against which it has been assessed and this Data Processing Annex.

4.2 In addition to the Reports, Processor shall respond to all reasonable requests for information made by Controller to confirm Processor's compliance with this Agreement, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Controller’s written request, provided that Controller shall not exercise this right more than once per calendar year.

4.3 Where the Processor is not audited against PCI standards, the Processor shall allow for audit inspections by Controller or Controller’s nominated consultant in order to assess compliance with this Agreement and Data Protection Laws. Processor shall also make available to

Controller all information reasonably necessary to demonstrate compliance with this Agreement and the Data Protection Laws.

4.4 In addition to the audit inspections, Processor, shall respond to all reasonable requests for information made by Controller or Controller's consultant to confirm Processor's compliance with the provisions of this Data Processing Annex, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Controller's or Controller's consultant written request.

5. *INTERNATIONAL TRANSFERS*

Controller acknowledges that Processor may transfer and process Personal Data outside of Nigeria where Processor, its Affiliates or its Sub-processors maintain data processing operations. Processor shall at all times ensure that such transfers are made in compliance with the requirements of Data Protection Laws.

6. RETURN OR DELETION OF DATA

Upon termination or expiration of the Agreement, Processor shall (at Controller's election) delete or return to Controller all Personal Data (including copies) in its possession or control, except that this requirement shall not apply to the extent Processor is required by applicable law to retain some or all of the Personal Data, or the Personal Data is archived on back-up systems, which Personal Data Processor shall securely isolate, protect from any further processing and eventually delete in accordance with Processor's deletion policies, except to the extent required by applicable laws.

7. DATA SUBJECT RIGHTS AND COOPERATION

7.1 Processor shall, taking into account the nature of the processing, provide reasonable additional assistance to Controller to the extent possible to enable Controller to comply with its data protection obligations with respect to a Data Subject's rights under Data Protection Laws.

7.2 If any request is made by a Data Subject to Processor directly, Processor shall not respond to such communication directly except as appropriate (for example, to direct the Data Subject to contact Controller) without Controller's prior authorisation except as legally required.

7.3 If Processor is required to respond to a request made under clause 7.2, Processor shall promptly notify Controller and provide Controller with a copy of the request unless Processor is legally prohibited from doing so. For the avoidance of doubt, nothing in this Data Processing Annex shall restrict or prevent Processor from responding to any Data Subject or data protection authority requests concerning Personal Data for which Processor is a controller.

7.4 If a law enforcement agency sends Processor a demand for Personal Data (for example, through a subpoena or court order), Processor shall attempt to redirect the law enforcement agency to request that Data directly from Controller. As part of this effort, Processor may provide Controller's contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then Processor shall give Controller reasonable notice of the demand to allow Controller to seek a protective order or other appropriate remedies, unless Processor is legally prohibited from doing so.

8. INDEMNIFICATION

8.1 The Processor agrees to indemnify, keep indemnified and defend at its own expense the Controller against all costs, claims, damages or expenses incurred by the Controller or for which the Controller may become liable due to any failure by the Processor or its employees, subcontractors or agents to comply with any of its obligations under this Data Processing Annex or the Data Protection Legislation.

8.2 Any limitation of liability provision outlined in the Agreement shall apply to the indemnity or reimbursement obligations in this Data Processing Annex.

9. RELATIONSHIP WITH THE AGREEMENT

9.1 This Data Processing Annex shall remain in effect for as long as Processor carries out Personal Data processing operations on behalf of Controller pursuant to the Agreement or until termination of the Agreement (and all Controller Data has been returned or deleted per clause 6 above).

9.2 The Parties agree that the provisions of this Data Processing Annex shall replace any existing data processing agreement or similar document that the Parties may have previously entered into in connection with the Service.

9.3 Except for any changes made by this Data Processing Annex, the Agreement remains unchanged and in full force and effect.

9.4 Notwithstanding anything to the contrary in the Agreement and this Data Processing Annex, Processor shall have a right to collect, use and disclose Data for its legitimate business purposes, such as: (i) for accounting, tax, billing, audit, and compliance purposes; (ii) to provide, develop, optimize and maintain the Service; (iii) to investigate fraud, spam, wrongful or unlawful use of the Service; and (iv) as required by applicable laws.

9.5 No one other than a party to the Agreement, its successors and permitted assignees shall have any right to enforce any of the terms of this Data Processing Annex.

10. GOVERNING LAW & DISPUTE RESOLUTION

10.1 This Data Processing Annex shall be governed by and construed in accordance with the laws of the Federal Republic of Nigeria.

10.2 Any dispute between the Parties in connection with the interpretation, implementation or operation of the Data Processing Annex or the validity of any document furnished by the

Parties shall be resolved in accordance with the dispute resolution provision in the Agreement.

11. SEVERABILITY

In the event any provision or part of this Data Processing Annex is found to be invalid or unenforceable, only that particular provision or part so found, and not the entire Data Processing Annex, will be inoperative.

12. NOTICES

Any notice or other communication given to a Party under or in connection with this Data Processing Annex must be in writing and delivered to:

For Interswitch Limited: 1648c Oko Awo Victoria Island, Lagos for the attention of Data Protection Officer.
Email: dpo@interswitchgroup.com

For User: via the electronic mail address or physical address Interswitch has on its records.