Jurisdiction	Nigeria
Date	5th April 2022
Law Firm	Udo Udoma and Belo-Osagie
Title, Name	Jumoke Lambo (Partner) Babatunde Olayinka (Senior Associate)
Contact Information	Name: Jumoke Lambo (Partner) Email: jumoke.lambo@uubo.org Tel: +234 1 2774920, 2719811, 2719812 +234 1 2774921, 2774922, 2719813 Mobile: +2348023133733 Name: Babatunde Olayinka (Senior Associate) Email: babatunde.olayinka@uubo.org Tel: +234 1 2774920, 2719811, 2719812 +234 1 2774921, 2774922, 2719813 Mobile: +234 8028951576

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the private sector at the present or in the near future? [Nigeria is yet to enact a principal legislation on data protection. Regardless, section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) ("the Constitution") guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. Further to this constitutional provision, the Nigeria Information Technology Development Agency ("NITDA") in January 2019 issued the Nigeria Data Protection Regulation 2019 ("NDPR") and the NDPR Implementation Framework ("Implementation Framework") in November 2020. The NDPR regulates the collection and processing of the Personal Data of Nigerian citizens and residents and protects such personal information.]

ii. Does your country have a general law concerning protection of personal information in the public sector at the present or in the near future? [See our response to i. above. Although Nigeria does not have a principal law, it has regulations that are of general application. Further to the issuance of the NDPR, the NITDA issued the Guidelines for the Management of Personal Data by the Public Institution in Nigeria (the "Guidelines") in 2020. The Guidelines provides guidance to public institutions in Nigeria on how to process and control Personal Data in compliance with the NDPR.]

iii. Does your country have laws concerning protection of personal information which

apply in individual (specific) sectors at the present or in the near future? (If yes, please describe outline.) [Yes, other than the NDPR and the NDPR Implementation Framework 2020 that applies generally in Nigeria, there are certain sector-specific regulations which regulate the processing of personal information in specific sectors of the economy such as the telecommunications, banking and the health sectors. These regulations include:

i. The Consumer Code of Practice Regulations 2007 (the "NCC Regulations"): The NCC Regulations was issued by the Nigerian Communications Commission ("NCC"), the regulator of the telecommunications sector in Nigeria. Part VI of the NCC Regulations generally deals with the protection of the personal information of customers in the telecommunications sector. Regulation 35 of the NCC Regulations provides that all NCC licensees must take reasonable steps to protect customer information against "improper or accidental disclosures" and must ensure that such information is securely stored. It also provides that customer information must "not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations".

ii. Registration of Telephone Subscribers Regulations 2011 ("Telephone Subscribers Regulations"): The Telephone Subscribers Regulations was issued by the NCC further to the Nigerian Communications Act. Regulation 9 of the Telephone Subscribers Regulations provides that further to the privacy rights guaranteed by section 37 of the Constitution of the Federal Republic of Nigeria, 1999 and subject to any guidelines issued by the NCC, including terms and conditions that may from time to time be issued either by the NCC or a licensee, any subscriber whose personal information is stored in the Central Database or a licensee's database, shall be entitled to view the said information and to request updates and amendments to such information whenever required. It further requires the subscriber's personal information that is stored in the central database to be held on a strictly confidentiality basis. It also provides in Regulation 5 that this information shall not be released to a third party or transferred outside Nigeria without the prior written consent of the subscriber and the NCC.

iii. The Consumer Protection Regulations 2020 ("the CBN Regulations"): The CBN Regulations was issued by the Central Bank of Nigeria (CBN) pursuant to the

Central Bank of Nigeria Act, 2007. Regulation 5.4 of the CBN Regulations provides for the protection of the privacy and confidentiality of consumer information and assets against unauthorized access and the accountability of institutions in the banking and finance sector for their acts or omissions in this respect. The written consent of consumers must be obtained before their personal data can be collected and processed for specific purpose and the consumers must be provided with the option to withdraw such consent at any time. Furthermore, institutions in the banking and finance sector cannot transfer the Personal Data of consumers to a third party without the express consent of the consumers, except where such transfer is in compliance with a legal obligation. These institutions are required to inform consumers whenever their Personal Data is exchanged with an authorized third party, stating details of such exchange. The institutions are also expected to carry out constant review of their data processing and privacy procedures to ensure that the purpose(s) for which the initial consent was granted remains valid. They are also required to keep accurate and updated data of consumers

iv. The National Health Act 2014 ("NHA"): Section 26 of the NHA restricts the disclosure of the personal information of users of health services in the records of any healthcare personnel or provider and requires them to take the necessary steps to protect the personal information of users of health services from unauthorised access.

v. The HIV and AIDS (Anti-Discrimination Act) 2014: Section 11(1) of the HIV and AIDS (Anti-Discrimination Act) 2014 prohibits employers from conducting HIV/AIDS tests on employees and employers may only carry out such tests where they have obtained the specific prior written consent of the employee. Where the employer is in possession of an employee's health information, which is considered to be sensitive personal data, the information must be held in strict confidence and can only be disclosed with the explicit consent of the employee.]

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information

mentioned at I (please add a reply column as necessary,)

The title of the law：Nigeria Data Protection Regulation 2019 (NDPR)

① The definition of “Personal Information”	The NDPR defines “Personal Data” as 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, an 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, Personal Identifiable Information (PII) and others.
② The scope in which the law applies	Based on Regulation 1.2 of the NDPR, the NDPR applies to: (i) all transactions intended for the processing of Personal Data, to the processing of Personal Data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria; and (ii) natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria. This means that the NDPR applies to the collection and processing of the Personal Data of all natural persons who reside in Nigeria and all natural persons who are Nigerian citizens residing outside Nigeria.
③ The territorial scope	The NDPR applies to the collection and processing of the Personal Data of all natural persons who reside in Nigeria. The NDPR also has extra-territorial impact because it applies to the processing of the Personal Data of Nigerian citizens who reside outside Nigeria.

The title of the law ：The Constitution of the Federal Republic of Nigeria 1999 (as amended)

① The definition of “Personal Information”	The Constitution does not define the phrase “personal information”.
② The scope in which the law applies	The Constitution applies to all Nigerian citizens.
③ The territorial scope	The constitution applies within Nigeria.

The title of the law ：The Guidelines for the Management of Personal Data by the Public Institution in Nigeria

④ The definition of	The Guidelines for the Management of Personal Data

	“Personal Information”	by the Public Institution in Nigeria defines “Personal Data” to mean any information allowing the identification of the Data Subject. This includes but not limited to information such as- name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, including but not limited to a name, address, a photo, an email address, bank details, posts on social networking websites or applications, medical information, and any other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others.
⑤	The scope in which the law applies	This Guidelines applies to all Public Institutions in Nigeria, including Ministries, Departments, Agencies, Institutions, Public Corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the Federal, State or Local levels, while processing the Personal Data of a Data Subject and operates for the purpose of the implementation of the NDPR.
⑥	The territorial scope	The Guidelines applies to the collection and processing of Personal Data by Nigerian public institutions in Nigeria.

The title of the law ：The Consumer Code of Practice Regulations 2007

⑦	The definition of “Personal Information”	The Regulation does not define the phrase “personal information”.
⑧	The scope in which the law applies	The Regulations apply to all NCC Licensees and any other providers of communication services in Nigeria.
⑨	The territorial scope	Nigeria

The title of the law ：Cybercrimes (Prohibition and Prevention etc.) Act 2015

⑩	The definition of “Personal Information”	There is no definition of the phrase “personal information” in the Cybercrimes Act.
⑪	The scope in which the law applies	This Act applies to cyber-crimes and related matters throughout the territory of Nigeria.
⑫	The territorial scope	Nigeria

The title of the law ： The Consumer Protection Regulations 2020

⑬	The definition of “Personal Information”	The Consumer Protection Regulations does not define the phrase “personal information”.
⑭	The scope in which the law applies	This Regulations applies to all institutions that are licensed and/or regulated by the Central Bank of Nigeria. Institutions ensures that the provisions of the Regulations form part of any consumer related transaction, product or service agreement they may

	enter into with any other institutions which are otherwise not regulated by CBN.
⑮ The territorial scope	Nigeria

The title of the law ：Registration of Telephone Subscribers Regulations 2011

⑯ The definition of “Personal Information”	The Regulation defines personal information to mean the full names (including mother’s maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of subscribers specified in the Registration Specifications.
⑰ The scope in which the law applies	These Regulations applies to all persons and licensees including: (a) corporate, private and commercial subscribers to Mobile Telephone Services utilising Subscription Medium in the Federal Republic of Nigeria ; and (b) subscribers of foreign licensees who are roaming on the network of a licensee in Nigeria. .
⑱ The territorial scope	Nigeria

The title of the law ：The HIV and AIDS (Anti-Discrimination Act) 2014

⑲ The definition of “Personal Information”	There is no definition of the phrase “personal information” in the HIV and AIDS (Anti-Discrimination Act).
⑳ The scope in which the law applies	The Act applies to all persons living with and affected by HIV and AIDS in Nigeria as well as all employers of labour and employees in the public and private sectors including the Nigeria Armed Forces, Nigeria Police, State Security Services, other Para Military Organisations, Schools, Hospitals and places of worship.
21 The territorial scope	Nigeria

The title of the law ：The National Health Act 2014

22 The definition of “Personal Information”	The National Health Act does not define the phrase “personal information”.
23 The scope in which the law applies	The Act applies to healthcare personnel or providers and generally the healthcare sector in Nigeria.
24 The territorial scope	Nigeria

ii. If there are any special instructions about the laws, please describe them.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle [The Collection Limitation Principle is captured in Regulation 2.1(1)(a) of the NDPR which requires the Personal Data of Data Subjects to be collected and processed in accordance with specific, legitimate and lawful purpose that is consented by the Data Subject. Regulation 2.1(1)(a)(i) further provides that further processing may only be done for archiving, scientific research, historical research or statistical purposes consented to by the Data Subject. Section 35(1)(a) of the Nigerian Communication Commission (NCC)'s Consumer Code of Practice Regulation 2007) also provides that the collection and maintenance of Personal Data by NCC licensees must be fair and lawful.]

(b) Data Quality Principle [The Data Quality Principle that states that Personal Data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date, is contained in Regulation 2.1(1)(b) of the NDPR which provides that the Personal Data being processed or to be processed must be adequate, accurate and without prejudice to the dignity of the human person.]

(c) Purpose Specification Principle [The principle of purpose specification in relation to data protection is encapsulated in Regulation 2.1(1)(a) of the NDPR which provides that the Personal Data obtained from the Data Subject shall only be processed in accordance with the specific, legitimate and lawful purpose consented to by the Data Subject. Regulation 3.1(7)(c) further mandates the Data Controller to provide the data subject with information relating to the purposes of the processing for which the Personal Data is intended as well as the legal basis for the processing of the Personal Data prior to collecting such Personal Data. Furthermore, where the Data Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data was collected, the Controller shall provide the Data Subject, prior to such further processing, with information on that other purpose, and with any relevant further information. Section 35 (1)(b) of the Consumer

Code of Practice Regulation provides that the collection and maintenance of Personal Data by NCC licensees must be for limited and identified purposes.]

(d) Use Limitation Principle [The principle of use limitation is expressed in Regulation 2.1(1)(a) of the NDPR which provides that the Personal Data obtained from the Data Subject shall only be processed in accordance with the specific, legitimate and lawful purpose consented to by the Data Subject. Regulation 3.1(7)(c) further mandates the Data Controller to provide the Data Subject with information relating to the purposes for which the Personal Data is intended to be processed, as well as the legal basis for the processing prior to collecting such Personal Data. In addition, where the Data Controller intends to further process the Personal Data for a purpose other than that for which the Personal Data was collected, the Controller shall provide the Data Subject, prior to that further processing, with information on that other purpose, and with any relevant additional information. Section 35 (1)(c) of the Nigerian Communication Commission (NCC)'s Consumer Code of Practice Regulation 2007) also embodies this principle by providing that the collection and maintenance of Personal Data by licensees must be relevant and not excessive.]

(e) Security Safeguards Principle [Regulation 2.1(1)(d) requires all Personal Data under the control of a Data Controller to be secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements. Regulation 2.6 of the NDPR also requires any person who is involved in the processing or control of Personal Data to develop security measures to protect the Personal Data. Such measures include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

Sections 35(1)(g) and (h) of the Consumer Code of Practice Regulation provides that the collection and maintenance of Personal Data by NCC licensees must be protected against improper or accidental disclosure and must not be transferred to any party except as permitted by any terms and

conditions agreed with the consumer, as permitted by any r approval of the NCC, or as otherwise permitted or required by other applicable laws or regulations.]

(f) Openness Principle [Regulation 2.1(1)(a) of the NDPR requires all Personal Data to be collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject. Also, the NDPR requires every medium through which Personal Data is collected or processed to display a simple and conspicuous privacy policy that the class of Data Subjects being targeted can understand. The NDPR also provides that privacy policies should contain the following information: (i) what constitutes the Data Subject's consent; (ii) a description of collectable personal information; (iii) purpose of collection of Personal Data; (iv) the technical methods used to collect and store personal information, cookies, JWT, web tokens etc.; (v) the access (if any) of third parties to Personal Data and purpose of access; (vi) a highlight of the principles of the NDPR; (vii) the available remedies in the event of violation of the privacy policy; and (viii) the time frame for remedy and any limitation clause, Regulation 3.1 of the NDPR also guarantees the right of the Data Subject to request access to their Personal Data and the Data Controller is obligated to take appropriate measures to provide, in writing or by other means, any information relating to processing of the Personal Data to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Where the Data Controller does not act on the request of the Data Subject, the Data Controller shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority. Furthermore, prior to collecting the Personal Data from the Data Subject, the Data Controller is to provide the identity and contact information of the Data Controller, Data Protection Officer, the recipients or categories of recipients of the Personal Data, and the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.]

(g) Individual Participation Principle [Under the NDPR, a Data Subject has and can exercise the following rights:

i. The Data Subject's right to access or obtain their Personal Data from the Data Controller. This right is guaranteed under Regulation 3.1 of the NDPR.

Under the NDPR, the Data Controller is required to take appropriate measures to provide any information relating to the processing of the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The NDPR also stipulates that a Data Controller has a maximum period of one month upon receipt of the Data Subject's request, to provide the information requested. The Data Controller is to ensure that the information is provided to the Data Subject free of charge. The Data Controller may, however, charge a reasonable fee to cover the administrative costs of providing the information requested by the Data Subject or may refuse to provide the information where the Data Subject's data access request is manifestly unfounded or excessive or is repetitive. The Data Controller may also write a letter to the Data Subject, copying the NITDA where it refuses to act on the data access request of the Data Subject.

ii. The Data Subject's right to object to the processing of his/her Personal Data is also provided under Regulation 2.8 of the NDPR, which states that a Data Subject is entitled to object to the processing of his/her Personal Data which the Data Controller intends to process for the purpose of marketing.

iii. The Data Subject's right to object to automated processing of their Personal Data. Paragraph 5.3.1 of the Implementation Framework provides that the Data Controller must obtain the consent of the Data Subject before the Data Controller makes a decision based solely on automated processing. Regulation 3.1(7)(l) also provides that prior to the processing of the Personal Data, the Data Subject ought to be informed of the existence of automated decision-making, including profiling and meaningful information should be provided to the Data Subject about the logic involved, the significance and the envisaged consequences of such processing for the Data Subject.

iv. The Data Subject also has the right to rectify any errors in his Personal Data and the right to be forgotten under the NDPR. Regulation 3.1(8) guarantees the right of a Data Subject to request the Data Controller, without undue delay, to rectify any inaccurate Personal Data concerning him or her. The Data Subject also has the right to request that his/her incomplete Personal Data be updated by providing supplementary statements. Regulation 3.1(8) of the NDPR grants the Data Subject the

right to request the Data Controller to delete his Personal Data without delay and the Data Controller is obligated to delete the Personal Data where any one of the following grounds applies:

- the Personal Data is no longer necessary in relation to the purposes for which they were collected or processed;
- the Data Subject withdraws consent on which the processing is based;
- the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the Personal Data have been unlawfully processed; and
- the Personal Data must be erased for compliance with a legal obligation in Nigeria.]

(h) Accountability Principle [Where a person is entrusted with or is in possession of the Personal Data of a Data Subject, Regulation 2.1(2) of the NDPR imposes a duty of care on such person to be accountable for his acts and omissions in respect of data processing in accordance with the principles contained in the NDPR. In addition, the NDPR requires data processing by a third party to be governed by a written contract between the third party and the Data Controller. Accordingly, any person engaging a third party to process the Personal Data obtained from Data Subjects is required to ensure the third party's strict adherence to the provisions of the NDPR.]

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

[We are not aware of any laws that exclude the application of the OECD principles as set out in the NDPR.

(a) Collection Limitation Principle

(b) Data Quality Principle

(c) Purpose Specification Principle

(d) Use Limitation Principle

(e) Security Safeguards Principle

(f) Openness Principle

(g) Individual Participation Principle

(h) Accountability Principle

IV. Data Localization and Government Access

i. In your country, are there any systems having an impact on the rights of data subjects such as comprehensive government access to personal data or Data Localization? If yes, please describe them.

[Yes. Government can have access to the Personal Data of citizens and residents under the control of Data Controllers in Nigeria. Under Regulation 2.2 of the NDPR, the legal bases upon which Personal Data can be processed lawfully include the following:

(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 Data Subject is 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 for the protection of 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.

Based on the foregoing, one of the legal bases for processing personal data is where the processing is necessary for compliance with a legal obligation to which the Controller is subject or where the processing is necessary for the performance of a task carried out in the public interest or in exercise of an official public mandate vested in the Controller. In view of this, government authorities in Nigeria, can access and process the Personal Data where such processing is necessary for the Data Controller's compliance with a legal obligation imposed on the Controller by

law or where such the processing is required for the performance of a task to be carried out in the public interest.

The NDPR Implementation Framework 2020 further excludes the following instances of processing of Personal Data from the scope of the NDPR:
(i) collection and processing of anonymised data;
(ii) personal or household activities with no connection to a professional or commercial activity;
(iii) investigation of criminal and tax offences; and
(iv) the use of Personal Data in furtherance of national security, public health, safety and order by agencies of the Federal, State or Local government or those they expressly appoint to carry out such duties on their behalf.

This means that security agencies and public authorities in Nigeria may request the disclosure of, or access to, Personal Data in furtherance of the investigation of a criminal or tax offence or in furtherance of national security, public health, safety and order.

Additionally, the Nigeria Communications Commission's Lawful Interception of Communications Regulations 2019 permits security agencies to intercept any communication relating to the use of communications service in Nigeria which is provided by a Licensee (that is, a telecommunications company) to persons in Nigeria, or require a Licensee to disclose any intercepted communication, pursuant to a judicial warrant. Such warrant must be issued in the interest of national security, for the purpose of preventing or investigating a crime, protecting and safeguarding the economic well-being of Nigerians, in the interest of public emergency or safety, or giving effect to any international mutual assistance agreement of which Nigeria is a party. However, this regulation applies specifically to companies that operate in the telecommunications sector in Nigeria.

Also, the Cybercrimes Act requires financial institutions to disclose personal information of cardholders upon request to the Central Bank of Nigeria or a licensed credit bureau. Service Providers (such as telecommunication companies) are also obliged to disclose any information requested by a law enforcement agency in any inquiry or proceeding under the Cybercrimes Act.

The NDPR does not have any specific data localisation provisions which requires Data Controllers and Data Processors to retain Personal Data in Nigeria. Personal Data can, therefore, be transferred outside Nigeria where the Data Controller meets the requirements for cross border transfer of Personal Data which is set out in the NDPR.

We should mention, however, that section 11.1(4) and 12.1(4) of the NITDA Guidelines for Nigerian Content Development in Information and Communication Technology ("NITDA ICT Guidelines") requires all telecommunications companies and network service companies to host all subscriber and consumer data in Nigeria.

In addition, Section 12.2(1) of the NITDA ICT Guidelines requires all government Ministries, Departments and Agencies to host all sovereign data locally on servers within Nigeria, whilst section 13.1(2) of the same guidelines requires all data and information management companies to also host all sovereign (government) data in Nigeria.

In addition, the Guidelines on Operations of Electronic Payment Channels in Nigeria ("CBN E-Payment Channels Guidelines") which was issued by the CBN in 2016 contains provisions that touch on data localisation in Nigeria. Section 2.4.4.8 of the CBN POS Guidelines requires all entities that engage in point of sale (POS) card acceptance services in Nigeria to use a local network switch (which connects devices and processes information to and from connected devices) for all domestic POS and ATM transactions. Also, domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers.

Similarly, section 2.4.1.6 mandates all Merchant Acquirers to switch all domestic transactions through a local switch for the purpose of seeking authorisation from the relevant issuer and such transactions should not under any circumstance be routed outside Nigeria. In relation to Mobile Point of Sale (mPOS), section 3.4.3.6 of the CBN E-Payment Channels Guidelines provides that all mPOS transactions must be switched using the services of a local switch and shall not under any circumstances be routed outside Nigeria.]

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority.

[The Nigeria Data Protection Bureau ("NDPB") has now replaced the NITDA as the data protection authority in Nigeria following the announcement on 4th February 2022, by the President of the Federal Republic of Nigeria, President Muhammadu Buhari of the establishment of NDPB as the dedicated data protection agency for Nigeria. The implication of this is that, going forward, the NDPB and not the NITDA will be responsible for the enforcement of data protection regulations and for the administration of all related data protection matters in Nigeria. However, until a substantive data protection legislation is enacted, the NDPB will continue to operate within the existing regulatory framework, that is, the NDPR and the NDPR Implementation Framework.

The NDPB is presently located within the NITDA, and its contact information is provided below:

No 28, Port Harcourt Crescent,

Off Gimbiya Street,

Area 11, Garki,

Federal Capital Territory, Abuja.]