International
Comparative
Legal Guides


Practical cross-border insights into data protection law

# Data Protection 2023

10th Edition

Contributing Editors:
**Tim Hickman & Dr. Detlev Gabel**
**White & Case LLP**

ICLG.com

# Expert Analysis Chapters



# Q&A Chapters

# Q&A Chapters Continued

# Nigeria



Jumoke Lambo


Chisom Okolie


Chidinma Chukwuma

Udo Udoma & Belo-Osagie


## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The principal data protection legislation in Nigeria is the Nigeria Data Protection Act 2023 ("NDPA") which was signed into law by President Bola Ahmed Tinubu on 14 June 2023.

### 1.2 Is there any other general legislation that impacts data protection?

The following laws and regulations impact data protection in Nigeria:

a. The Constitution of the Federal Republic of Nigeria 1999 (as amended).
b. The Nigeria Data Protection Regulation 2019 ("NDPR").
c. The NDPR Implementation Framework 2020, issued by the National Information Technology Development Agency ("NDPR Implementation Framework").
d. The Child Rights Act 2003.
e. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
f. The Freedom of Information Act, 2011.
g. The National Health Act, 2014.
h. The HIV and AIDS (Anti-Discrimination) Act, 2014.

### 1.3 Is there any sector-specific legislation that impacts data protection?

The following sector-specific laws, regulations and guidelines have an impact on data protection in Nigeria:

a. The Consumer Code of Practice Regulations 2007 ("NCC Regulations, 2007") published by the Nigerian Communications Commission ("NCC").
b. The Registration of Telephone Subscribers Regulations 2011, published by the NCC.
c. The Consumer Protection Regulations 2020, issued by the Central Bank of Nigeria ("CBN"), Nigeria's apex bank.
d. The Lawful Interception of Communications Regulations, 2019 which was issued by the NCC.
e. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020, issued by the NITDA.
f. The Official Secrets Act 1962.
g. The CBN Guidelines on Point of Sale Card Acceptance Services 2011.
h. The CBN Regulatory Framework for Bank Verification Number Operations and Watch-List for The Nigerian Banking Industry 2017.
i. The NITDA Guidelines for Nigerian Content Development in Information and Communication Technology 2019 (as amended).
j. The Credit Reporting Act 2017.

### 1.4 What authority(ies) are responsible for data protection?

The Nigeria Data Protection Commission ("NDPC") is the primary data protection authority and is responsible for enforcing the NDPA in Nigeria. The NDPA establishes the NDPC. The NDPC is the agency responsible for enforcing the provisions of the NDPA and the administration of all data protection matters in Nigeria. The NDPA retained and did not repeal the existing NDPR and its Implementation Framework. These documents are now to be read in conjunction with the NDPA; however, where there is any conflict in their provisions, the provisions of the NDPA are to prevail.

Sector-specific regulatory authorities like the CBN and the NCC may also enforce the various regulations that touch on data protection within the sectors that they regulate.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  The NDPA defines "Personal Data" as any information relating to an individual, who can be identified or is identifiable, directly or indirectly, in particular 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, physiological, genetic, psychological, cultural, social or economic identity of that individual.

- "**Processing**"
  The NDPA defines "Processing" as any operation or set of operations which is performed on 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, and does not include the mere transit of data originating outside Nigeria.
- "**Controller**"
  According to the NDPA, a "Data Controller" is an individual, private entity, public Commission or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Data Controller or Data Processor of Major Importance**"
  According to the NDPA, a "Data Controller or Data Processor of Major Importance" is a Data Controller or Data Processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the NDPC may prescribe, or such other class of Data Controller or Data Processor that is processing Personal Data of particular value or significance to the economy, society or security of Nigeria as the NDPC may designate.
- "**Processor**"
  According to the NDPA, a "Data Processor", is an individual, private entity, public authority, or any other body, who processes Personal Data on behalf of or at the direction of a Data Controller or another Data Processor.
- "**Data Subject**"
  The NDPA defines a "Data Subject" as an individual to whom personal data relates.
- "**Sensitive Personal Data**"
  Under the NDPA, "Sensitive Personal Data" means Personal Data relating to an individual's:
  - genetic and biometric data for the purpose of uniquely identifying a natural person;
  - race or ethnic origin;
  - religious or similar beliefs, such as those reflecting conscience or philosophy;
  - health status;
  - sex life;
  - political opinions and affiliations;
  - trade union membership; or
  - other information prescribed by the NDPC as Sensitive Personal Data.
- "**Data Breach**"
  According to the NDPA, a "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.
- **Other key definitions**
  "**Pseudonymisation**"
  According to the NDPA, "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.
  The NPDA and the NDPR do not recognise the concepts of "Direct Personal Data" or "Indirect Personal Data".
  The NDPR also provides for the following key definitions:
  "**Automated Decision-Making**": means a decision based solely on automated processing by automated means, without any human involvement.
  "**Binding Corporate Rules**": means personal data protection policies and procedures adhered to by the members of a group of firms under common control with respect to the transfer of personal data among such members and containing provisions for the protection of such personal data.
  "**Data Portability**": The NDPR defines Data Portability as the ability of data to be transferred easily from one IT system or computer to another through a safe and secured means in a standard format.
  "**Data Protection Compliance Organisation**": This refers to an entity duly licensed by the NDPC for the purposes of training, auditing, consulting and rendering services and products to ensure compliance with the NDPA or any foreign data protection law that has effect in Nigeria.
  "**Data Subject Access Request**": Under the NDPR, this means the mechanism for an individual to request a copy of their personal data under a formal process which may include the payment of a fee.

## 3 Territorial Scope

**3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?**

According to Section 2(2) of the NDPA, the NDPA will apply to businesses established in other jurisdictions where the businesses are involved in the processing of the Personal Data of Data Subjects in Nigeria.

## 4 Key Principles

**4.1 What are the key principles that apply to the processing of personal data?**

- **Transparency**
  Section 24(1) of the NDPA provides that Personal Data shall be processed in a fair, lawful and transparent manner. It also provides that Personal Data is to be collected for specified, explicit, and legitimate purposes and is not to be further processed in a way incompatible with these purposes.
- **Lawful basis for processing**
  Section 25 of the NDPA provides six lawful bases for the processing of Personal Data:
  a. where the Data Subject has given and not withdrawn consent for the specific purpose or purposes for which Personal Data is to be processed;
  b. where processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
  c. where processing is necessary for compliance with a legal obligation to which the Data Controller or Data Processor is subject;

d. where processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
e. where processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the Data Controller; or
f. where processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or Data Processor, or by a third party to whom the data is disclosed.

- **Purpose limitation**
The principle of purpose limitation in relation to data protection is set forth in Section 24(1)(b) of the NDPA, which provides that a Data Controller or Data Processor shall ensure that Personal Data is collected for specified, explicit and legitimate purposes, and not to be further processed in a way that is incompatible with these purposes.
- **Data minimisation**
Section 24(1)(c) of the NDPA requires Data Controllers or Data Processors to ensure that Personal Data is adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed. Therefore, a Data Controller, when processing Personal Data, must ensure that the Personal Data is adequate and relevant for the purpose(s) for which it is being processed.
- **Proportionality**
Please see our answer to the question on Data minimisation above.
- **Retention**
Section 24(1)(d) of the NDPA provides that a Data Controller or Data Processor shall ensure that Personal Data is retained for not longer than is necessary to achieve the lawful bases for which the Personal Data was collected or further processed. Section 8.2 of the NDPR Implementation Framework specifies the statutory retention periods for storing Personal Data which will be applicable where no specific duration is agreed between parties or is stated in any applicable law. The retention period stipulated in section 8.2 of the NDPR Implementation Framework are as follows:
  a. three years after the last active use of a digital platform;
  b. six years after the last transaction in a contractual agreement;
  c. upon the presentation of evidence of death by a deceased's relative, the Data Controller and/or Processor must immediately delete the Personal Data of the deceased Data Subject unless there is a legal obligation imposed on the Data Controller to continue to store the Personal Data;
  d. immediately upon a request by the Data Subject or his/her legal guardian where:
    i. no statutory provision provides otherwise; and
    ii. the Data Subject is not the subject of an investigation or suit that may require the Personal Data sought to be deleted.

  The NDPR Implementation Framework further requires that Personal Data which is no longer in use or which has been retained beyond the requisite statutorily required retention period be destroyed in line with global best practices for such operations.
- **Other key principles**
The NDPA also recognises the following principles:
**Data Security**: Section 24(1)(f) provides that a Data Controller or Data Processor shall ensure that Personal Data is processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach. Section 39(1) also requires a Data Controller and Data Processor to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of Personal Data in its possession.
**Accountability**: Section 24(3) provides that a Data Controller or Data Processor owes a duty of care, in respect of data processing, and shall demonstrate accountability, in respect of the principles contained in the NDPA. In addition, the NDPA 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 terms of such written contracts and the provisions of the NDPA.

## 5 Individual Rights

### 5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
The Data Subject's right to access their Personal Data or copies of such data is guaranteed under Section 34(1)(b) of the NDPA. Under the NDPA, a Data Subject has the right to obtain from a Data Controller, without constraint or unreasonable delay a copy of the Data Subject's Personal Data in a commonly used electronic format, except to the extent that providing such data would impose unreasonable costs on the Data Controller, in which case the Data Subject may be required by the Data Controller to bear some or all of such costs. Regulation 3.1 of the NDPR also provides that the Data Controller is required to take appropriate measures to provide any information relating to the data processing to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This will also apply to information relating to a child. The information is to be provided in writing, or by other means (including electronically or orally, provided that the identity of the Data Subject is proven by some other means, where the information is to be provided orally).
The NDPR also stipulates a maximum period of one month within 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 NDPC where it refuses to act on the data access request of the Data Subject.
- **Right to rectification of errors**
Section 34(1)(c) of the NDPA guarantees the right of a Data Subject to request that the Data Controller, correct or if not feasible or suitable, delete the Data Subject's Personal Data that is inaccurate, out of date, incomplete or misleading.
Under Regulation 3.1(13) of the NDPR, the Data Controller shall also communicate any rectification to each recipient to whom the Personal Data have been disclosed unless this

proves impossible or requires a disproportionate effort. The Data Controller is also obligated to inform the Data Subject about those recipients if the Data Subject requests for this disclosure.

- **Right to deletion/right to be forgotten**
  Section 34(1)(d) of the NDPA provides that a Data Subject has the right to request for the erasure of Personal Data concerning the Data Subject, without undue delay. Section 34(2) of the NDPA also provides that the Data Controller shall erase Personal Data without undue delay, where:
  i. the Personal Data are no longer necessary in relation to the purposes for which they were collected or processed; or
  ii. the Data Subject has no other lawful basis to retain the Personal Data.
  Regulation 3.1(10) of the NDPR requires the Data Controller who has made the Personal Data public to take all reasonable steps to inform the Data Controllers who are processing the Personal Data of the Data Subject's request to delete the data.
  Under Regulation 3.1(13) of the NDPR, the Data Controller is required to also communicate any erasure of Personal Data to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The Data Controller is also obligated to inform the Data Subject about those recipients if the Data Subject requests it.
- **Right to object to processing**
  Section 36 of the NDPA provides that a Data Subject is entitled to object to the processing of his/her Personal Data. It also provides that the Data Controller shall discontinue the processing of Personal Data, unless the Data Controller demonstrates a public interest or other legitimate grounds, which overrides the fundamental rights and freedoms, and the interests of the Data Subject.
- **Right to restrict processing**
  Section 34(1)(v) of the NDPA provides that the Data Subject has the right to request for the restriction of processing of its Personal Data or to object to such processing.
  Regulation 3.1(11) of the NDPR provides that the Data Subject is entitled to restrict the Data Controller's processing of his/her Personal Data where one of the following applies:
  i. The accuracy of the Personal Data is contested by the Data Subject for a period enabling the Data Controller to verify the accuracy of the Personal Data.
  ii. The processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead.
  iii. The Data Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims.
  iv. The Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.
  Regulation 3.1(12) also provides that where processing has been restricted, such Personal Data shall, except for the purpose of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest in Nigeria.
  Under Regulation 3.1(13), the Data Controller shall also communicate any restriction on the processing of Personal Data to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or requires a disproportionate effort. The Data Controller is also obligated to inform the Data Subject about the recipients of his/her data where the data Subject requests for such information.
- **Right to data portability**
  Section 38 of the NDPA gives the Data Subject the right to Data Portability. It entitles him/her to:
  (a) receive Personal Data from a Data Controller in a structured, commonly used, and machine-readable format;
  (b) transmit Personal Data to another Data Controller without any hindrance; and
  (c) have the Personal Data transmitted directly from one Data Controller to another, where technically possible.
- **Right to withdraw consent**
  Section 35 of the NDPA provides that a Data Subject shall have the right to withdraw, at any time, consent to the processing of his/her Personal Data. The Data Controller is to ensure that it is as easy for the Data Subject to withdraw, as to give consent. The withdrawal of consent shall not affect the lawfulness of data processing that occurred before the withdrawal of the consent. Section 26(4) of the NDPA also provides that where the processing of Personal Data is based on the consent of the data subject, the data subject shall be informed of the right to withdraw consent, prior to the granting of consent.
- **Right to object to marketing**
  Section 36(3) of the NDPA provides that where Personal Data is processed for direct marketing purposes, the data subject shall have the right to object, at any time, to the processing of the Personal Data concerning the data subject, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.
- **Right to be informed of the existence of automated decision-making and profiling**
  Section 27(g) of the NDPA provides that before a Data Controller collects Personal Data directly from a Data Subject, the Data Controller shall inform the Data Subject of the existence of automated decision-making, including profiling, significance, and envisaged consequence of such processing for the data subject, and the right to object to and challenge such processing. Section 37 of the NDPA also provides that Data Subject's shall have the right not to be subject to a decision based solely on automated processing of Personal Data, including profiling, which produces legal or similar significant effects concerning the data subject.
- **Right to complain to the relevant data protection authority(ies)**
  Data Subjects are entitled under 34 of the NDPA to lodge a complaint with the NDPC.
- **Other key rights**
  Under Regulation 3.1(8) of the NDPR, where Personal Data are transferred to a foreign country or to an international organisation, the Data Subject has the right to be informed of the appropriate safeguards for protecting his/her Personal Data in such foreign country.

**5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.**

According to Regulation 4.1(8) of the NDPR, the mass media and civil societies may uphold accountability and foster the objectives of the NDPR. Section 9.1 of the NDPR Implementation Framework provides that, in addition to Data Subjects and government agencies, civil societies or professional organisations may also report a breach of the NDPR to the NDPC.

## 6 Children's Personal Data

**6.1 What additional obligations apply to the processing of children's personal data?**

Under the NDPA, for the purpose of processing Personal Data, a child is any person below the age of 18. Section 31 of the NDPA requires Data Controllers to apply appropriate mechanisms to verify age and consent, taking into consideration available technology. The presentation of any government-approved identification documents is sufficient for this purpose. Section 31(5) of the NDPA also empowers the NDPC to make regulations relating to the processing of the Personal Data of a child of 13 years and above in relation to the provision of information and services by electronic means at the specific request of the child.

Where the processing activity of the Data Controller or Processor targets children, section 5.5 of the NDPR Implementation Framework imposes an obligation on the Data Controller or Processor to ensure that its privacy policy is made in a child-friendly form with the aim of making the children and their parents/guardians have a clear and easy understanding of the data processing activity before granting their consent to the processing of their child/ward's Personal Data.

Furthermore, Regulation 2.4(a) of the NDPR prohibits Data Controllers from seeking or accepting consent for processing Personal Data in any circumstance that may violate or endanger a child's rights.

## 7 Registration Formalities and Prior Approval

**7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?**

The NDPA, requires Data Controllers and Data Processors of Major Importance to register with the NDPC within six months after the commencement of the NDPA or on becoming Data Controllers and Data Processors of Major Importance. As the NDPA was passed into law on 14 June 2023, the NDPC has not yet provided a definition of who a Data Controller or Data Processor of Major Importance is, neither has it provided any guidance in relation to this issue.

The NDPR also requires Data Controllers or Processors to conduct a detailed audit of their privacy and data protection practices and on an annual basis, submit a summary of their data protection audit to the NDPC no later than 15 March of the following year where the Data Controller or Processor has processed the Personal Data of more than 2,000 Data Subjects in a period of 12 months. Data Controllers and Processors who process the Personal Data of Data Subjects are required to comply with the provisions of the NDPR.

**7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?**

In order for Data Controllers and Data Processors of Major Importance to be registered with the NDPC, they are required to provide the following information:

a. the name and address of the Data Controller or Data Processor, and the name and address of the Data Protection Officer ("DPO") of the Data Controller or Data Processor;
b. the description of Personal Data and the categories and number of Data Subjects to which the Personal Data relate;
c. the purposes for which Personal Data is processed;
d. the categories of recipients to whom the Data Controller or Data Processor intends or is likely to disclose Personal Data;
e. the name and address of any representative of any Data Processor operating directly or indirectly on its behalf;
f. the country to which the Data Controller or Data Processor intends, directly or indirectly to transfer the Personal Data;
g. a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the Personal Data; and
h. any other information required by the NDPC.

With respect to the filing of the Data Controller or Processor's data protection compliance audit report with the NDPC, Regulation 4.1(5) of the NDPR requires the report to contain the following information:

a. personally identifiable information the organisation collects on employees of the organisation and members of the public;
b. any purpose for which the personally identifiable information is collected;
c. any notice given to individuals regarding the collection and use of personal information relating to that individual;
d. any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
e. whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
f. the policies and practices of the organisation for the security of personally identifiable information;
g. the policies and practices of the organisation for the proper use of personally identifiable information;
h. the organisation's policies and procedures for privacy and data protection;
i. the policies and procedures of the organisation for monitoring and reporting violations of privacy and data protection policies; and
j. the policies and procedures of the organisation for assessing the impact of technologies on the stated privacy and security policies.

### 7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please see our answer to question 7.1 above.

### 7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Local entities who are Data Controllers or Data Processors of Major Importance will be required to register with the NDPC. The NDPA defines a "Data Controller or Data Processor of Major Importance" as a Data Controller or Data Processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process Personal Data of more than such number of data subjects who are within Nigeria, as the NDPC may prescribe, or such other class of Data Controller or Data Processor that is processing Personal Data of particular value or significance to the economy, society or security of Nigeria as the NDPC may designate. It is not yet clear whether the NDPC will also require foreign entities to register and we await further guidance on this issue from the NDPC.

### 7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see our answer to question 7.3 above.

### 7.6 What are the sanctions for failure to register/notify where required?

Sections 48 and 49 of the NDPA provide that the NDPC may impose fines in respect of a breach of the provisions of the NDPA. The range of fines imposed under the NDPA are as follows:

a. in the case of a Data Controller or Data Processor of Major Importance, the payment of a fine of 2% of the organisation's annual gross revenue of the preceding year or the payment of the sum of 10 million Naira, whichever is greater; and
b. in the case of a Data Controller or Data Processor not of Major Importance, the payment of a fine representing 2% of the organisation's annual gross revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater.

In addition, Section 48 of the NDPA states that the NDPC may also issue enforcement orders including: requiring the Data Controller or Data Processor to remedy the violation; ordering the Data Controller or Data Processor to pay compensation to a Data Subject; ordering the Data Controller or Data Processor to account for the profits realised from the violation, or harm as a result of a violation; or referring the matter to the appropriate regulatory agencies for sanction and to prosecute the organisation.

The NDPC may also institute criminal proceedings where it has determined that an organisation is in breach of the provisions of the NDPA or NDPR, especially where such breach affects national security, sovereignty and cohesion. The NDPC may also seek a fiat of the Honourable Attorney General of the Federation or may file a petition with any authority in Nigeria. This may include: the Economic and Financial Crimes Commission; the Department of State Security; the Nigerian Police Force; Independent Corrupt Practices (and other related offences) Commission; or the Office of National Security Adviser.

### 7.7 What is the fee per registration/notification (if applicable)?

In relation to filing the data protection compliance audit, Section 6.3 of the Implementation Framework prescribes the audit filing fees as 10,000 Naira for Data Controllers with less than 2,000 Data Subjects and 20,000 Naira for Data Controllers or Processors with more than 2,000 Data Subjects, respectively.

The NDPC is yet to provide any guidance in relation to the fees that will be applicable for the registration of Data Controllers or Data Processors of Major Importance.

### 7.8 How frequently must registrations/notifications be renewed (if applicable)?

The NDPC is yet to provide any guidance in relation to the frequency of the registration/renewal of registration as a Data Controller or Data Processor of Major Importance.

### 7.9 Is any prior approval required from the data protection regulator?

Prior approval is not required from the NDPC to conduct and file a data protection compliance audit.

### 7.10 Can the registration/notification be completed online?

Yes. Filing of data-protection-compliance audit reports can be done online through the web portal of the NDPC. Section 44 of the NDPA requires Data Controllers and Data Processors of Major Importance to be registered with the NDPC within six months after commencement of the NDPA or on becoming a Data Controller and Data Processor of Major Importance. However, the NDPC has not issued any guidance in relation to how the registration will be carried out.

### 7.11 Is there a publicly available list of completed registrations/notifications?

The NDPC, on a yearly basis, publishes a list of organisations that comply with the annual data protection audit and filed their audit report with the NDPC.

### 7.12 How long does a typical registration/notification process take?

The filing of a data-protection-compliance audit report with the NDPC on the online platform can be completed within a day and upon the payment of the applicable filing fees.

## 8 Appointment of a Data Protection Officer

**8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.**

Section 32 of the NDPA provides that a Data Controller of Major Importance shall designate a DPO with expert knowledge of data protection law and practices, and the ability to carry out the tasks prescribed under the NDPA and subsidiary legislation made under it.

Regulation 4.1 of the NDPR and Section 3.4.1 of the Implementation Framework also mandate every Data Controller to designate or appoint a DPO for the purpose of ensuring adherence to the NDPA, relevant data privacy instruments and data protection directives of the Data Controller.

In addition, an organisation that is based in Nigeria would be required to appoint a dedicated DPO who is resident in Nigeria and has full access to the management team in Nigeria, if the organisation falls within the following categories of Data Controllers:

a. the entity is a government organ, Ministry, Department, institution or Agency;
b. the core activities of the organisation involve processing Personal Data of over 10,000 Data Subjects per annum;
c. the organisation processes Sensitive Personal Data in the regular course of its business; or
d. the organisation possesses critical national information infrastructure (as defined under the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 or any amendment thereto) consisting of Personal Data.

**8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?**

The penalties stated in question 7.6 above are applicable.

**8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?**

The DPO is usually an employee or an external organisation contracted to act in this capacity. As a result, the DPO would be bound by the terms of its employment contract or any contract for service that relates to disciplinary measures or other employment consequences.

**8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?**

Yes. A business may appoint a single DPO to cover multiple entities. We should, however, mention that section 3.5 of the Implementation Framework mandates a Nigerian subsidiary of a multinational company to appoint a Nigerian-based DPO, and the DPO of the Nigerian subsidiary may report to a global DPO where such exists.

**8.5 Please describe any specific qualifications for the Data Protection Officer required by law.**

Section 32(3) of the NDPA provides that a DPO shall:

a. advise the Data Controller or the Data Processor, and their employees, who carry out processing made under the NDPA;
b. monitor compliance with the NDPA and related policies of the Data Controller or Data Processor; and
c. act as the contact point for the NDPC on issues relating to data processing.

Section 3.7 of the Implementation Framework also provides that a DPO should be chosen with due regard to the nature of the business's processing activities and data protection issues. It further lists the qualities of the DPO to include:

a. having professional expertise in Nigerian data protection laws and practices;
b. having an in-depth understanding of applicable data protection laws; and
c. having the requisite knowledge to do the following:
    i. inform and advise the organisation, management, employees and third-party processors of their obligations under the NDPR and the NDPA;
    ii. monitor compliance with the NDPR, the NDPA and with the organisation's own data protection objectives;
    iii. assign responsibilities, raise awareness and train members of staff involved in Personal Data processing activities and operations;
    iv. advice on data protection impact assessment and monitor its performance; and
    v. liaise with the NDPC and/or the DPCO on data protection matters.

**8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?**

Please see our answer to question 8.5 above.

**8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No. It is not mandatory that the NDPC is notified when an organisation appoints a DPO.

**8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?**

Regulation 3.1(7) of the NDPR lists the identity and contact details of the DPO as part of the information a Data Controller is required to provide to the Data Subject before collecting his/her Personal Data. Therefore, the DPO should be identified in the Data Controller's privacy policy, notice or any equivalent document.

## 9 Appointment of Processors

**9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?**

Yes. Section 29(2) of the NDPA requires a Data Controller to enter into a written contract (i.e. a third-party data processing contract) with a third party ("Third-Party Processor") where it engages that third party to process the Personal Data obtained from Data Subjects on its behalf.

**9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?**

A third-party data processing contract is required to be written, signed and must expressly state the roles and obligations of the Data Controller and Third-Party Processor including processing data only upon the authorisation of the Data Controller, securing data, complying with Data Subjects Access Requests amongst other matters.

## 10 Marketing

**10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).**

Yes. By virtue of the provision of Section 5.3.1 of the NDPR Implementation Framework, the consent of the Data Subject is required for direct marketing except where the direct marketing activity is targeted at existing customers of the Data Controllers who have purchased goods or services.

Section 36(4) of the NDPA provides that where the Data Subject objects to processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

**10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?**

We are of the opinion that the above restriction will apply to both contexts if they involve the processing of Personal Data of natural persons who are Data Subjects within the provisions of the NDPA. This is because the provisions of the NDPA apply only to the processing activities of the Personal Data of natural persons; that is to say, a Data Subject under the NDPA is a natural person and not a business entity.

**10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).**

Please see our answer to question 10.1.

**10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?**

Yes, they would apply to marketing that is sent from other jurisdictions where the Personal Data of Nigerian citizens and residents will be processed for such marketing activity. Marketing sent from another jurisdiction implies that the marketers already have the Personal Data of their targets (Data Subjects) which means there had been a prior transfer of the data to that other jurisdiction. For such transfer to have been possible, the Data Subject must have consented to the transfer of his/her Personal Data and also to the use or purpose of such transfer.

**10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?**

Yes. The breach of these marketing restrictions is a breach of the provisions of the NDPA, and the NDPC has the responsibility of enforcing penalties for any breaches of the provisions of the NDPA.

**10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?**

No, it is not lawful to purchase marketing lists from third parties except where the Data Subject gives his/her consent to the processing of his/her Personal Data for marketing purposes and to transfer of his/her Personal Data to such third parties. Where a Data Controller intends to transfer the Personal Data of a Data Subject, such Data Controller must ensure that it obtains the consent of the Data Subject according to the provisions of the NDPR.

**10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?**

The NDPA has a general penalty provision which would also apply where marketing communications are sent in breach of the provisions of the NDPA. Section 49 of the NDPA, in addition to criminal prosecution, prescribes the following penalties for anyone who is found to be in breach of the data privacy rights of any Data Subject:

a. in the case of a Data Controller or Data Processor of Major Importance, payment of a fine of 2% of its annual gross revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater; and
b. in the case of a Data Controller or Data Processor not of Major Importance, payment of the fine of 2% of its annual gross revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater.

## 11 Cookies

**11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).**

According to section 5.6 of the Implementation Framework, the

use of cookies on a website requires consent. A website owner is required to:

a. make the cookie information clear and easy to understand;
b. notify users of the presence and purpose of the cookies;
c. identify the entity responsible for the use of the cookies; and
d. provide information on how to withdraw consent from the use of the cookie.

**11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?**

The NDPR does not distinguish between different types of cookies.

**11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?**

We are not aware of any enforcement action that has been taken by the NDPC in relation to cookies.

**11.4 What are the maximum penalties for breaches of applicable cookie restrictions?**

Please see our answer to question 10.7.

## 12 Restrictions on International Data Transfers

**12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.**

Please refer to question 7.1 above.

**12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).**

In Nigeria, Personal Data can be transferred outside Nigeria in the following circumstances:

a. the recipient of the Personal Data is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection with respect to the Personal Data in accordance with the NDPA.
b. the Data Subject has provided and not withdrawn the consent to such transfer after having been informed of the possible risks of such transfers for the Data Subject due to the absence of adequate protection;
c. the transfer is necessary for the performance of a contract to which a Data Subject is a party or in order to take steps at the request of a Data Subject, prior to entering into a contract;
d. the transfer is for the sole benefit of a Data Subject; and
    i. it is not reasonably practical to obtain the consent of the Data Subject to that transfer; and
    ii. if it were reasonably practicable to obtain such consent, the Data Subject would likely give it;
e. the transfer is necessary for important reasons of public interest;
f. the transfer is necessary for the exercise or defence of legal claims; or
g. the transfer is necessary to protect the vital interests of a Data Subject or of other persons, where a Data Subject is physically or legally incapable of giving consent.

Section 42 of the NDPA also provides that a level of protection is adequate if it upholds principles that are substantially similar to the conditions for processing of the Personal Data provided for in this Act. The adequacy of protection shall be addressed taking into account the:

a. availability of enforceable Data Subject rights, the ability of a Data Subject to enforce such rights through administrative or judicial redress, and the rule of law;
b. existence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection;
c. access of a public authority to Personal Data;
d. existence of an effective data protection law;
e. existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and
f. international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.

**12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.**

No registration/notification or prior approval is required to transfer Personal Data to other jurisdictions. Sections 41 of the NDPA provide that Personal Data can be transferred outside Nigeria where the recipient of the Personal Data is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection with respect to the Personal Data in accordance with the NDPA.

Section 42 of the NDPA also provides that a level of protection is adequate if it upholds principles that are substantially similar to the conditions for processing of the Personal Data provided for in this Act. The adequacy of protection shall be addressed taking into account the:

a. availability of enforceable Data Subject rights, the ability of a Data Subject to enforce such rights through administrative or judicial redress, and the rule of law;
b. existence of any appropriate instrument between the Commission and a competent authority in the recipient jurisdiction that ensures adequate data protection;
c. access of a public authority to Personal Data;
d. existence of an effective data protection law;
e. existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and
f. international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations.

Data Controllers are therefore not required to notify the NDPC or any other regulator where they intend to transfer a Data Subject's Personal Data to other jurisdictions so long as they rely on the above-mentioned bases for transfer.

However, the NDPC has the power to make regulations requiring Data Controllers and Data Processors to notify it of the measures in place to ensure adequacy of protection when transferring a Data Subject's Personal Data to a foreign country.

**12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?**

This is not applicable to Nigeria.

**12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?**

This is not applicable to Nigeria.

## 13 Whistle-blower Hotlines

**13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?**

There are no restrictions on the type of issues that may be reported. Any action amounting to a breach of the NDPA may be reported. According to section 46 of the NDPA, a Data Subject who is aggrieved by the decision, action or inaction of a Data Controller or Data Processor in violation of the NDPA, or subsidiary legislation made under the NDPA may lodge a complaint with the NDPC.

**13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?**

Anonymous reporting is generally permitted.

## 14 CCTV

**14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?**

The NDPA applies 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. The Use of CCTV does not require a separate registration or prior approval from the NDPC but should ideally be brought to the attention of the Data Subject. The improper use of CCTV can result in a breach of privacy rights. It is recommended that a notice stating that CCTVs are being used should be placed in a conspicuous part of the facility, such as the entrance so everyone is aware that CCTVs are being used.

**14.2 Are there limits on the purposes for which CCTV data may be used?**

Yes, the Data obtained can only be used for the purpose stated in the CCTV privacy policy.

## 15 Employee Monitoring

**15.1 What types of employee monitoring are permitted (if any), and in what circumstances?**

The NDPA did not specifically make provisions for employee monitoring. The NDPA, however, applies to any kind of transaction in which the processing of Personal Data of Nigerian residents is being carried out. Any monitoring activity carried out by the employer on the employee should either be pursuant to a provision in their contract of employment or notice should be given to the employees and their consent obtained before such monitoring is carried out. Such monitoring should not be covert.

**15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

The consent of the employees must be obtained in accordance with the NDPA before the employee monitoring may take place. Under the NDPA, the consent of the Data Subject must be a freely given, specific, informed and unambiguous indication whether by a written or oral statement or an affirmative action, of the Data Subject's agreement to the processing of Personal Data relating to him/her or to another individual on whose behalf he/she has the permission to provide such consent. Consent is required to be obtained from the Data Subject without fraud, coercion or undue influence, and prior to obtaining such consent, the specific purpose of collection of the Personal Data must be made known to the Data Subject.

According to Regulation 2.3(2)(b) of the NDPR, where the Data Subject's consent is given via a written declaration which also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Prior to granting his/her consent, the Data Subject is also required to be notified of his/her right and method to withdraw his/her consent at any given time. Consent cannot be implied, i.e., inactivity or silence does not constitute consent. Section 5.4 of the Implementation Framework further specifies the types of consent that are acceptable under the NDPR. It provides that consent can be explicit consent or an opt-in consent. Explicit consent is given where the Data Subject provides a clear and documentable agreement, e.g. ticking a box, signing a form, sending an email or signing a paper or document. Opt-in consent, on the other hand, refers to a situation where consent can only be said to have been given when the Data Subject chooses to opt in to the processing of his/her Personal Data.

The employees should, therefore, be informed of the kind of monitoring schemes that are in place and the purpose for such monitoring activity, and the employers must ensure that the consent of the employees to monitoring must be express, and freely given in accordance with the provisions of the NDPA, the NDPR and the Implementation Framework.

**15.3 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?**

The employer has no obligation under the data protection laws to inform trade union on the steps it takes to monitor its employee unless it is a provision of a collective bargaining or other agreement with the trade union.

**15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?**

Employers can process information on an employee's COVID-19 vaccination status in the following instances:

a. when the employee consents to such processing;
b. where the processing is necessary for the purposes of performing the obligations of the employers or exercising rights of the employees under employment or social security laws;
c. where the processing is necessary to protect the vital interests of the employee or of another person, where the employee is physically or legally incapable of giving consent;
d. where the processing is carried out in the course of the employer's legitimate activities, with appropriate safeguards, by a foundation, association, or such other not-for-profit body with charitable, educational, literary, artistic, philosophical, religious, or trade union purposes, and:
    i. the processing relates solely to the members or former members of the entity, or to persons, who have regular contact with it in connection with its purposes; and
    ii. the Sensitive Personal Data is not disclosed outside of the entity without the explicit consent of the data subject,
e. the processing relates to Personal Data, which are manifestly made public by the employee;
f. the processing is necessary for the establishment, exercise, or defence of a legal claim, obtaining legal advice, or conduct of a legal proceeding;
g. the processing is necessary for reasons of substantial public interest, on the basis of a law, which shall be proportionate to the aim pursued, and provides for suitable and specific measures to safeguard the fundamental rights and freedoms and the interests of the employee;
h. the processing is carried out for purposes of medical care or community welfare, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality;
i. the processing is necessary for reasons of public health and provides for suitable and specific measures to safeguard the fundamental rights and freedoms, and the interests of the employee; or
j. the processing is necessary for archiving purposes in the public interest, or historical, statistical, or scientific research, in each case on the basis of a law, which shall be proportionate to the aim pursued, and provides for suitable and specific measures to safeguard the fundamental rights and freedoms and the interests of the employee.

## 16 Data Security and Data Breach

**16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?**

Yes, there is. According to Section 39 of the NDPA, a Data Controller and Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of Personal Data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure or access. Hence, both the Data Controller and the Data Processor have the obligation to secure Personal Data. Where data is being transferred to a third party, such transfer will be governed by a contract between both the Data Controller and the third party. The contract will spell out the role of both the Data Controller and the third party in relation to the protection of the data of the Data Subject. It is important to note that under the NDPA, the Data Controller who engages the services of third-party processors remains primarily liable to the Data Subjects for the protection of the Personal Data it collects.

**16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Yes. There is a legal requirement to report a breach to the data protection authority. Section 40 of the NDPA provides that a Data Controller or Processor is expected to report any incidence of a breach to the NDPC within 72 hours of becoming aware of the breach. This timeline is required to be documented in the organisation's data protection policy and data privacy policy. The details to be reported include:

a. A description of the nature of the Personal Data breach including the categories and approximate number of Data Subjects and Personal Data records concerned.
b. The name and contact details of a point of contact of the Data Controller, where more information can be obtained.
c. A description of the likely consequences of the Personal Data breach.
d. A description of the measures taken or proposed to be taken to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.
e. A description of steps the organisation has taken to reduce the risk of harm to individuals.

**16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what**

**timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.**

Under Section 40(3) of the NDPA, the Data Controller is required to immediately notify the Data Subject of a Personal Data breach where the breach will likely result in high risks to the freedoms and rights of the Data Subject.

**16.4 What are the maximum penalties for data security breaches?**

The penalties stated in question 7.6 above are applicable.

## 17 Enforcement and Sanctions

**17.1 Describe the enforcement powers of the data protection authority(ies).**

a. **Investigative Powers:** Without prejudice to the right of a Data Subject to approach a court of competent jurisdiction for the breach of his/her privacy rights, the NDPC can initiate the investigation of allegations of any breach of the provisions of the NDPA where it appears to it that the complaint is not frivolous or vexatious. It can invite any party to respond to allegations made against it.
b. **Corrective Powers:** Where the NDPC has ascertained that a Data Controller or Data Processor has violated or is likely to violate any requirement under the NDPA or subsidiary legislation, the NDPC may issue an order for compliance with relevant provisions to curtail further breaches.
c. **Authorisation and Advisory Powers:** The NDPC can issue administrative orders to protect the subject-matter of an allegation pending the outcome of investigation.
d. **Imposition of administrative fines for infringements of specified NDPA provisions:** The NDPC has the power to issue a monetary fine after completing an investigation and being satisfied that a Data Controller or Data Processor has violated any provision of the NDPA or subsidiary legislation. A decision on the money value shall be based on the following considerations:
    i. the nature, gravity and severity of the breach;
    ii. the number of data subjects affected;
    iii. the purpose of the processing;
    iv. the level of damage and damage mitigation measures implemented;
    v. the intent or negligence;
    vi. the degree of cooperation with the NDPC; and
    vii. the types of personal data involved.
e. **Non-compliance with a data protection authority:** Any person who is found to be in breach of the data privacy rights of any Data Subject will be liable, in addition to any other criminal liability, to:
    i. In the case of a Data Controller or Data Processor of Major Importance – a monetary fine of 2% of the Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater.
    ii. In the case of a Data Controller or Data Processor not of Major Importance – a fine of 2% of the Annual Gross Revenue of the preceding year or the sum of 2 million Naira, whichever is greater.

**17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?**

The NDPC being the data protection authority has the power to make orders for suspension of service by the Data Controller (including processing activities) pending further investigations.

**17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.**

When the NDPR was issued in 2019, the attitude of the NITDA was to increase awareness of the regulation and encourage compliance. However, recently there appears to be a shift in the NITDA/NDPC approach and the NDPC seems to have adopted an enforcement-based approach. For example, in August 2021, the NITDA announced that it had fined Soko Lending Company Limited a sum of 10 million Naira for various violations of the NDPR. We are also aware that the NDPC, sometime in February, announced that it was investigating a total of 110 companies for various violations of the NDPR. The NDPC has not issued the outcome of these investigations.

**17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?**

We are not aware of any extra-territorial enforcement of the NDPA or any decided case law against a foreign company that was based on the provisions of the NDPR. Having said this, we understand that the NDPC is looking to develop a framework document for extra-territorial enforcement of the NDPA through collaboration with other data protection agencies outside Nigeria. We do not know when this will be achieved.

We should also mention that we are aware that the NITDA, in 2019, investigated certain allegations against some foreign companies who allegedly processed the Personal Data of Nigerian citizens or residents in contravention of the provisions of the NDPR. Please see https://www.vanguardngr.com/2019/09/were-investigating-truecaller-over-breach-of-privacy-rights-nitda/.

We are also aware that the interagency Joint Regulatory and Enforcement Task Force ("JRETF"), which comprises the Federal Competition and Consumer Protection Commission, the NDPC, the Central Bank of Nigeria, the Economic and Financial Crimes Commission and the Independent Corrupt Practices Commission, is investigating the practices of digital money lenders in Nigeria and in August 2022, the JRETF issued orders against Google and Apple to take down the Apps of some digital money lenders from their respective App Stores.

## 18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

**18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?**

Businesses respond positively to such request subject to the provisions of the NDPA.

**18.2 What guidance has/have the data protection authority(ies) issued?**

We are not aware of whether the NDPC has issued any guidance pertaining to data protection matters.

## 19 Trends and Developments

**19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.**

Ove the last few months, the NDPC has announced that it has commenced investigations of about 110 companies (including banks, loan sharks, consulting firms and a telecommunications firm) for potential breaches of the data privacy of their customers.

The NDPC is yet to announce the outcome of these investigations.

**19.2 What "hot topics" are currently a focus for the data protection regulator?**

This is not applicable to Nigeria.

## Acknowledgments

The authors acknowledge Uchechukwu Ojimba and Yaknse Ekanem for their contributions to this chapter.

**Jumoke Lambo** is a Partner at Udo Udoma & Belo-Osagie. She heads the Telecommunications, Media and Technology team ("TMT") (which includes Data Protection), and she co-heads the firm's Aviation, Corporate Advisory and Employment (which includes Immigration and Business Establishment) teams.
She also oversees Alsec Nominees Limited, the firm's company secretarial practice. Jumoke was admitted to the Nigerian Bar in 1989 and obtained an LL.B. degree from University of Bristol in 1988. She joined Udo Udoma & Belo-Osagie as an Associate in 1989, became a Senior Associate in 1998 and made Partner in 2000.
Jumoke has over three decades' experience in telecommunications law, data protection, cybersecurity, employment law, immigration law and general corporate practice with an emphasis on corporate advisory, legislative drafting, mergers and acquisitions, foreign investment, corporate restructuring, regulatory compliance and due diligence.
Jumoke is recognised by the Nigerian edition of *Who's Who Legal* for her M&A practice. Her work has also been noted in the *International Financial Law Review*'s *Expert Guides*. She was recognised in December 2020 by *Business Day Newspaper* as one of Nigeria's top 20 female lawyers in business law. Jumoke is also a Notary Public.

**Udo Udoma & Belo-Osagie**
St. Nicholas House (10th ,12th and 13th Floors)
Catholic Mission Street
Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: jumoke.lambo@uubo.org
URL: www.uubo.org

**Chisom Okolie** is an Associate in the firm's TMT, Corporate Finance and Energy teams. As a professional who understands the law and how it applies to clients' businesses, she has advised on various areas of the law including: data protection; debt financing; private equity; corporate re-structuring and mergers and acquisitions; energy; telecommunications, media and technology; and entertainment practice.
Chisom has co-authored articles in the *International Comparative Legal Guide* series, *Thomson Reuters Practical Law Journal*, and has been recognised for her contributions to the World Bank Group's *Doing Business Guide* as well as its *Women, Business and the Law Report*. Due to her continued contributions to the finance and energy sectors, she received a national award as a "Nigerian Rising Star" and one of the "40 leading lawyers under the age of 40" in Nigeria and a "key lawyer" recognition by top international legal ranking bodies such as the *International Financial Law Review* and *The Legal 500*.

**Udo Udoma & Belo-Osagie**
St. Nicholas House (10th ,12th and 13th Floors)
Catholic Mission Street
Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: chisom.okolie@uubo.org
URL: www.uubo.org

**Chidinma Chukwuma** is an Associate in the firm's TMT, Private Equity and Mergers and Acquisitions teams. She has advised on various areas of the law including: data protection; private equity; intellectual property; mergers and acquisitions; banking and finance; and TMT.
Chidinma has also been recognised for her contributions to the World Bank Group's *Women, Business and the Law Report*.

**Udo Udoma & Belo-Osagie**
St. Nicholas House (10th ,12th and 13th Floors)
Catholic Mission Street
Lagos Island, Lagos
Nigeria

Tel: +234 1 2774920 / +234 1 2719811 / +234 1 2719812
Email: chidinma.chukwuma@uubo.org
URL: www.uubo.org

# ICLG.com

## Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group