International Comparative Legal Guides

Data Protection 2020

A practical cross-border insight into data protection law

Seventh Edition

Featuring contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Chandler MHM Limited
Clyde & Co
DDPV Studio Legale
Deloitte Kosova Shpk
Deloitte Legal Shpk
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
Elzaburu S.L.P.
FABIAN PRIVACY LEGAL GmbH
Herbst Kinsky Rechtsanwälte GmbH
Homburger AG
Khaitan & Co LLP
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners
LPS L@w
LYDIAN
Marval O'Farrell Mairal
Matheson
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
NEOVIAQ IP/ICT
Nyman Gibson Miralis
OLIVARES
Pellon de Lima Advogados
PPM Attorneys
Rothwell Figg
Semenov&Pevzner
SEOR Law Firm
SKW Schwarz Rechtsanwälte
SSEK Indonesian Legal Consultants
S. U. Khan Associates Corporate & Legal Consultants
Synch Advokatpartnerselskab
Templars
White & Case LLP
White & Case, s.r.o., advokátní kancelář
Wikborg Rein Advokatfirma AS

ICLG.com

Expert Chapters

Q&A Chapters

Q&A Chapters Continued

Nigeria


Emmanuel Gbahabo


Oghomwen Akpaibor

Templars

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Nigeria's principal data protection legislation is the Nigeria Data Protection Regulation 2019 ("**NDPR**"). The NDPR was issued by the National Information Technology Development Agency ("**NITDA/the Agency**") on 25 January 2019 pursuant to Section 32 of the NITDA Act 2007 as subsidiary legislation to the NITDA Act 2007. The Act establishes the Agency, the official Government body that develops and regulates information technology in Nigeria.

In July 2019, NITDA released a draft NDPR Implementation Framework ("**NDPRIF**") the purpose of which is to ensure the effective implementation and enforcement of the NDPR. Although the NDPRIF is currently in draft form, most of the provisions of the Framework are currently being employed by the Agency in the interim, in order to facilitate a proper implementation of the NDPR pending the final document being released.

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

Other general legislation which impacts data protection includes:

- The Constitution of the Federal Republic of Nigeria, 1999 (as amended) (the "**Constitution**"): Section 37 thereof guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic materials.
- The Freedom of Information Act, 2011: This provides for the duty of public institutions to make information available to any person who applies for it, but Section 14 thereof expressly excludes information that relates to private or personal data of individuals from the category of information to be so made available.
- The Child's Right Act 2003: Section 8 thereof provides for the right to privacy of a child in Nigeria.
- The Nigerian Communications Commission ("**NCC**") Act, 2003: The NCC has issued several regulations pursuant to this Act which impact data protection in the telecommunication industry (see question 1.3 below).
- The National Identity Management Commission ("**NIMC**") Act 2007: Section 26 of the Act mandates prior authorisation of the NIMC before accessing data or information contained in the National Identity Database.
- The Cybercrime (Prohibition, Prevention, Etc.) Act 2015 ("**Cybercrime Act**"): This Act criminalises cybercrimes in Nigeria. Sections 14 and 16 thereof prohibit dealing with data stored in a computer system or network in a fraudulent manner for fraudulent purposes. Section 19 thereof requires financial institutions to protect customer data, while Section 12 thereof prohibits unlawful interception of electronic communications.
- The HIV and AIDS (Anti-Discrimination) Act 2014: Section 13(1) thereof grants all persons living with HIV or affected by AIDS the right to protection of data with respect to their health and medical records.

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

- The Central Bank of Nigeria ("**CBN**") Act 2007: Pursuant to this Act, the CBN issued the Consumer Protection Framework 2016 which requires financial institutions to ensure adequate protection of customer data.
- National Health Act 2014: This Act requires health establishments to maintain and ensure the confidentiality of health records of every user of health services.
- The Credit Reporting Act 2017: Section 9 thereof guarantees the right of data subjects under the Act to privacy and confidentiality with respect to their credit information held by credit bureaux.
- The Consumer Code of Practice Regulations 2007 issued by the NCC require licensees in the telecommunications sector to ensure adequate protection of customer information.
- The Registration of Telephone Subscribers Regulations 2011 issued by the NCC provide for the confidentiality of records of telephone subscribers maintained in the NCC's central database.

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

The following authorities are responsible for data protection in Nigeria:

- NITDA.
- NCC.
- NIMC.
- CBN.
- Federal Ministry of Health.

2 Definitions

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

- "**Personal Data**"
  This means any information relating to an identifiable natural person. An identifiable natural person is one who can be identified, 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, an address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as, but not limited to, the MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information ("**PII**") and others.
- "**Processing**"
  This means any operation which is performed on personal data by automated means, such as collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**"
  The NDPR defines a "data controller" as a person who either alone, jointly with other persons or in common with other persons or a statutory body, determines the purposes for and the manner in which personal data is processed or is to be processed.
- "**Processor**"
  The NDPR does not define "processor" but defines a data administrator as a person or an organisation that processes data.
- "**Data Subject**"
  This means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.
- "**Sensitive Personal Data**"
  This means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal record or any other sensitive personal information.
- "**Data Breach**"
  The NDPR defines a "Personal Data Breach" as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")

- "**Data Subject Access Request**" means a mechanism for an individual to request a copy of their data under a formal process and payment of a fee.
- "**Data Portability**" means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format.
- "**Third Party**" means any natural or legal person, public authority, establishment or any other body other than the data subject, the data controller, the data administrator and the persons who are engaged by the data controller or the data administrator to process personal data.
- "**Consent**" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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?

The NDPR applies to businesses established in other jurisdictions. The effect of Section 1.2 of the NDPR is that a business established in another jurisdiction would be subject to the NDPR where such business undertakes transactions that involve the processing of the personal data of natural persons residing in Nigeria, or outside of Nigeria but of Nigerian descent.

4 Key Principles

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

- **Transparency**
  The specific purpose of data collection must be made known to the data subject before obtaining personal data. Section 2.3(1) of the NDPR. Para. 8.2(a) of the NDPRIF.
- **Lawful basis for processing**
  Section 2.2 of the NDPR states that processing shall be lawful if at least one of the following applies:
  a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
  b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
  c) processing is necessary for compliance with a legal obligation to which the controller is subject;
  d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; and
  e) processing is necessary for the performance of a task carried out in the public interest or in exercise of an official public mandate vested in the controller.
- **Purpose limitation**
  Personal data is to be collected and processed in accordance with a specific, legitimate, and lawful purpose consented to by the data subject. Further processing of personal data may be done only for archiving, scientific research, historical research, or statistical purposes for public interest. Section 2.1 of the NDPR.
- **Data minimisation**
  The NDPR provides that only adequate/necessary personal data should be collected and should be stored only for the period within which it is reasonably needed. Section 2.1(1)(b) and (c) of the NDPR.
- **Proportionality**
  By virtue of Section 45(1) of the Constitution, any provision of any law which purports to restrict or limit the constitutional right to privacy must be reasonably justifiable in a democratic society in the interest of defence, public safety,

public order, public morality or public health, or for the purpose of protecting the rights and freedom of other persons.

- **Retention**
  Section 2.1(1)(c) of the NDPR provides that personal data should be stored only for the period within which it is reasonably needed. Section 38 of the Cybercrime Act requires service providers to keep traffic data and subscriber information for two years thereof. Section 5 of the Credit Reporting Act 2017 also requires credit bureaux to maintain credit information for not less than six years from the date of obtaining such information, after which such information is to be archived for 10 years and may thereafter be destroyed. Reg 35 (1) (e) of the NCC Consumer Code of Practice Regulations 2007 requires licensees not to keep information on individual consumers for a period that is longer than necessary.

Other key principles – please specify

- **Data Security**
  Section 2.1(d) of the NDPR requires that personal data should 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.
  Also, Section 19.3 of the Cybercrime Act requires financial institutions to put in place effective counter-fraud measures to safeguard sensitive information.

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**
  A data subject has the right to request access to his or her personal data provided to the data controller. Section 3.1(7)(h) of the NDPR.
- **Right to rectification of errors**
  A data subject has the right to rectify his or her personal data. Section 3.1(7)(h) of the NDPR.
- **Right to deletion/right to be forgotten**
  A data subject has the right to request the deletion and erasure of his or her personal data, subject to the provisions of the NDPR. Section 3.1(7)(h) and 3.1(9) of the NDPR.
- **Right to object to processing**
  A data subject has the right to object to processing of his or her personal data. A data subject also has the right to be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge. Section 2.8 of the NDPR.
- **Right to restrict processing**
  A data subject has the right to restrict processing of his or her personal data. Section 3.1(7)(h) and (11) of the NDPR. Where processing has been restricted, such personal data shall, except for 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. Section 3.12 of the NDPR.
- **Right to data portability**
  A data subject has the right to data portability. In exercising this right, the data subject has the right to have his or her personal data transmitted directly from one controller to another, where technically feasible. Section 3.15 of the NDPR.
- **Right to withdraw consent**
  A data subject has the right to be informed of his or her right and method to withdraw his or her consent at any time. A withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Section 2.3(2)(c) of the NDPR and Section 8.3 of the NDPRIF.
- **Right to object to marketing**
  A data subject has the right to object to the processing of his or her personal data for the purpose of marketing. Section 2.8(a) of the NDPR.
- **Right to complain to the relevant data protection authority(ies)**
  A data subject has the right to seek redress in a court of competent jurisdiction or by lodging a complaint with NITDA for breach of his or her data privacy rights. Sections 2.10 and 4.2 of the NDPR.

Other key rights – please specify

- **Right to receive information related to processing, free of charge**
  A data subject has the right to receive from a data controller, any information relating to processing of his or her personal data provided to such controller, in a concise, transparent, intelligible and easily accessible form, using clear and plain language under Section 3.1(1) of the NDPR. Except where such requests for information are manifestly unfounded or excessive, and except as otherwise provided by any public policy or regulation, such information are to be provided free of charge. Section 3.1(3) of the NDPR.
- **Right to receive data in a machine-readable format**
  A data subject has the right to receive his or her personal data which has been provided to a data controller, in a structured, commonly used and machine-readable format. Section 3.1(14) of the NDPR.

6 Registration Formalities and Prior Approval

6.1 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 NDPR does not mandate registration or notification of processing activities of businesses with NITDA. It does, however, specify that a data controller who processes the personal data of more than 2,000 subjects in a period of 12 months is to submit a summary of its data protection audit to NITDA not later than 15 March of the following year. Section 4.1(6) and (7) of the NDPR.

Further, a data controller who processes the personal data of more than 1,000 subjects in a period of six months is to submit a soft copy of the summary of its data protection audit to NITDA.

The NDPR also mandates the registration and licensing of organisations that qualify as Data Protection Compliance Organisations ("**DPCOs**"). DPCOs are organisations which on behalf of the Agency are responsible for monitoring, auditing, conducting training and data protection compliance consulting to all data controllers under the NDPR. Section 4.1(4) of the NDPR.

6.2 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)?

No registration or notification of processing activities is required. Only data controllers processing personal data of between 1,000

and 2,000 Nigerians or persons living in Nigeria are required to submit audits to NITDA. By virtue of Section 4.1(5) and (6) of the NDPR, the details which must be specified in the audit to be submitted to NITDA by a data controller are as follows:

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. organisation 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.

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

Notifications in the form of annual audits submitted by data controllers to NITDA are to be made on the basis of a database threshold, i.e. where a data controller processes personal data of more than 1,000 subjects in a period of six months or where a data controller processes personal data of more than 2,000 subjects in a period of 12 months. Section 4.1(6) and (7) of the NDPR.

6.4 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)?

Although only entities designated as DPCOs are required to be registered/licensed by NITDA, the NDPR requires every data controller to designate or appoint a Data Protection Officer for the purpose of ensuring adherence to the NDPR, relevant data privacy instruments and data protection directives of the data controller. The data controller through the Data Protection Officer therefore has the duty of filing the requisite annual audits with the authorities. Section 4.1(2) and 4.1(4) of the NDPR.

6.5 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 the answer to question 6.2 above.

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

The NDPR does not contain specific sanctions for failure to register or notify NITDA of activities for which notification/registration is required. However, pursuant to Section 17(4) of the NITDA Act 2007, an individual or body corporate that fails to comply with the guidelines and standards prescribed by NITDA commits an offence punishable by: a fine of ₦200,000 or imprisonment for one year or both fine and imprisonment, for a first offence; and a fine of ₦500,000 or imprisonment for three years or both fine and imprisonment, for second and subsequent offences.

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

Notification or filing fees for annual audit reports required to be filed by data controllers to NITDA depend on the number of data subjects processed by the data controller.

a. Less than 10,000 data subjects: ₦5,000 (approx. US$14).
b. Between 10,000–50,000 data subjects: ₦10,000 (approx. US$28).
c. More than 50,000 data subjects: ₦20,000 (approx. US$56).

As regards DPCOs, registration with NITDA is free; however, a licensing fee of ₦50,000 is payable by DPCOs to NITDA on an annual basis.

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

The NDPR requires notification/filing of audit to be made annually. Section 4.1(7) of the NDPR. DPCOs are also required to pay for their licensing fees annually.

6.9 Is any prior approval required from the data protection regulator?

Only DPCOs require prior approval from NITDA in the form of registration and licensing. Section 4.1(4) of the NDPR.

6.10 Can the registration/notification be completed online?

The NDPR does not provide for online registration/notification.

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

No, the list of data controllers who have filed their annual audit is not publicly available. However, the list of duly licensed DPCOs is available publicly via the NITDA website.

6.12 How long does a typical registration/notification process take?

Filing of the annual audit by the data controller typically takes approximately one to two weeks, barring any administrative delays and provided all relevant documents are submitted by the data controller.

7 Appointment of a Data Protection Officer

7.1 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.

Appointment of a Data Protection Officer is only mandatory for organisations that act as data controllers under the NDPR. Please refer to question 2.1 above for the definition of a data controller.

Furthermore, Para. 3.2 of the NDPRIF specifies certain instances where appointment of a DPO is necessary, as follows:

a) the entity is a Government Organ, Ministry, Department, Institution or Agency;
b) the core activities of the organisation relate to usual processing of large sets of personal data;
c) the organisation processes sensitive personal data in the regular course of its business; and
d) the organisation processes critical national databases consisting of personal data.

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

There is no specific penalty for failure to appoint a Data Protection Officer, but failure to comply with the NDPR is generally treated as a breach of the NITDA Act, which may attract fines and possible criminal penalties upon conviction. A first offence attracts a fine of ₦200,000 (approx. US$555) or imprisonment for a term of one year, or both a fine and imprisonment. Subsequent offences attract a fine of ₦500,000 (approx. US$1,387) or imprisonment for a term of three years, or both.

7.3 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 NDPR does not provide any protection or immunity for Data Protection Officers.

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

The NDPR does not restrict a business from appointing a single Data Protection Officer for multiple entities, provided strict adherence to the requirements of the Regulation is maintained across the board.

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

There are no specific qualifications required by law, but Data Protection Officers are expected to have verifiable competence, usually in the form of certification or training in data protection, security and privacy.

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

Data Protection Officers are expected to ensure that their organisation maintains compliance with the NDPR and any other data protection laws, regulations or directives. The officer is to advise the organisation on compliance requirements and obligations, monitor internal policies to ensure they are in tandem with the NDPR, encourage continuous capacity-building for data protection, mandate a publicly available privacy policy for the organisation in compliance with the NDPR, and facilitate the cooperation of staff in maintaining compliance. The officer would also act as the primary point of liaison with NITDA. Importantly, the Data Protection Officer should ensure submission of annual audit reports duly certified by a DPCO, to NITDA as required by the NDPR.

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

No; as stated above, only DPCOs are required to register with NITDA.

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

There is no strict legal requirement for this, but it may be beneficial to do so. This is because the NDPR requires that prior to collecting personal data from a data subject, the controller shall provide the data subject with the contact details of the Data Protection Officer. Thus, if the public privacy notice/policy is all a data subject sees prior to consenting to the collection of data, then our view is that the details of the Data Protection Officer should be present in such notice, policy or equivalent document.

8 Appointment of Processors

8.1 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, businesses are required to have written agreements with third-party processors. Section 2.7 of the NDPR.

8.2 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.)?

The NDPR mandates that the agreement should be in writing. We would generally expect parties to contract in writing and in accordance with due execution under Nigerian contract law. The NDPR does not go into exact specifics as to what the agreement must address, but it does prescribe that it should be drafted in accordance with the NDPR. Thus, such agreements should ordinarily contain provisions for lawful processing of data, data privacy/security, third-party transfer, etc. and that parties are required to take reasonable measures to ensure that the other party does not have a record of violating the principles set out in Part 3 of the NDPR (on the rights of a data subject).

9 Marketing

9.1 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?).

The NDPR protects the right if a data subject objects to the processing of his or her data for marketing purposes. The NDPR also specifies that the data controller must provide a mechanism for objection to the data subject. Section 2.8 of the NDPR.

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

The Regulation does not provide any distinction between one and the other.

9.3 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.).

The NDPR does not provide any such restrictions but the NCC Consumer Code of Practice Regulations restricts telemarketing by telecommunication companies in Nigeria. Certain disclosures must be made to subscribers prior to such marketing: (i) the third party making the communication; (ii) the purpose of the communication; (iii) the full price of the product or service being marketed; and (iv) confirmation that the individual retains the right to cancel the agreement to purchase or lease within seven days of the telemarketing communication. Additionally, the NCC has a do-not-disturb code in force which enables subscribers to activate it and prohibit unsolicited marketing messages.

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

Marketing restrictions under the NDPR would apply to marketing from other jurisdictions as long as they are targeted at Nigerians or persons residing in Nigeria. On the other hand, marketing restrictions under the NCC regulations apply to NCC Licensees and, by extension, would apply to foreign marketing where such marketing activities are executed by local operators or telecommunications providers on behalf of the foreign entity.

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

The NCC is the most active regulator in this regard. NITDA is fairly new and enforcement measures are yet to take full effect, especially in view of the current COVID-19 pandemic.

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

The NDPR does not speak to this specifically, but the general principle on obtaining consent of the data subject would apply. Additionally, the NCC Consumer Code of Practice Regulations and Registration of Telephone Subscribers Regulation prohibit telecommunication service providers from providing third parties with access to subscribers' data. It is possible that this prohibition may be overridden by consent of the data subject/subscriber, but this has yet to be tested.

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

The NDPR does not prescribe any specific penalties in this regard; however, a breach by a data controller in terms of failure to provide adequate mechanisms for objection to processing for marketing purposes would be a breach of the NDPR, which ultimately constitutes a breach of the NITDA Act. Failure to comply with the NDPR is generally treated as a breach of the NITDA Act, which attract fines and possible criminal penalties upon conviction. A first offence attracts a fine of ₦200,000 (approx. US$555) or imprisonment for a term of one year, or both a fine and imprisonment. Subsequent offences attract a fine of ₦500,000 (approx. US$1,387) or imprisonment for a term of three years, or both.

Under the Nigerian Communications (Enforcement Processes, etc.) Regulations 2005, breach of marketing restrictions attracts a fine of ₦10,000,000 (approx. US$27,740).

10 Cookies

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

The NDPR and the NDPRIF provide some restrictions on cookies. The use of cookies on a website or digital platform requires consent of the data subject/user accessing the website/platform. Consent must be freely given, informed and specific. The consent must not be express – continued usage of a website which meets the prescribed requirements is sufficient consent (the requirements are: clear and easily understood information on cookies; purpose for use of cookies must be provided; identity of person responsible for cookies must appear; and consent must be capable of being withdrawn). Para. 8.4 of the NDPRIF and Section 2.5(d) of the NDPR.

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

No. However, the NDPRIF specifies under Para. 5.0 that the NITDA website uses encrypted session cookies.

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

We are not aware of any such enforcement action having been taken by NITDA.

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

There are no specific penalties for breach of applicable cookie restrictions, but failure to comply with the NDPR may generally

be treated as a breach of the NITDA Act, which may attract fines and possible criminal penalties upon conviction. A first offence attracts a fine of ₦200,000 (approx. US$555) or imprisonment for a term of one year, or both a fine and imprisonment. Subsequent offences attract a fine of ₦500,000 (approx. US$1,387) or imprisonment for a term of three years, or both.

11 Restrictions on International Data Transfers

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

Transfer of data to other jurisdictions is required to take place under the supervision of the Office of the Honourable Attorney General of the Federation ("**HAGF**"), which is expected to assist NITDA in prescribing a whitelist of countries with sufficient data protection laws that are acceptable for cross-border transfer. However, such whitelist is yet to be prescribed.

In the absence of this, the applicable exceptions under the NDPR are:

- consent of the data subject after being informed of the possible risks of transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11.2 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.).

Businesses would typically procure the consent of the data subject, being the most common and easiest means to navigate the AG's supervision for transfer of data cross-border. Also, clauses in contractual arrangements may specify the requirements for transfer of data outside of Nigeria in the performance of the contract or for any other legitimate purpose.

11.3 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.

Transfer of personal data does not require registration/notification or prior approval from NITDA. However, the same must be done under the supervision of the HAGF. What is required is that the data be transferred to a jurisdiction which has been whitelisted by NITDA (under the supervision of the HAGF) or, in the absence of any decision having been made as to the satisfactoriness of that jurisdiction, the transfer is made within the exceptions detailed in question 11.1 above.

12 Whistle-blower Hotlines

12.1 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.)?

The NDPRIF advocates reporting of data breaches by data controllers and administrators.

Also, Para. 5.1.2 of the NDPRIF specifies that a compliance officer or any person who believes a party is not complying with any of the provisions of any regulatory instrument may file a complaint with NITDA. Such complaints must meet the following requirements:

a. A complaint must be filed in writing, either on paper or electronically.
b. A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable provision(s).
c. NITDA may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing.

That said, it must be noted that Nigeria currently does not have substantive whistle-blowing legislation. There are some sector-specific whistle-blowing policies, and the Federal Ministry of Finance has a federal whistle-blowing programme in respect of stolen/misappropriated funds, but whistle-blowing as a whole is outside the scope of the data protection laws and legislation currently in force in Nigeria.

12.2 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 in whistleblowing policies in Nigeria; however, such a complaint must state the name of the subject of the complaint in accordance with the NDPRIF.

13 CCTV

13.1 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)?

No, there is no specific requirement under the NDPR for prior registration/notification or prior approval from NITDA for the use of CCTV. However, the use of CCTV comes under the purview of the NDPR as it is a medium through which PII is collected (including pictures or videos, as the case may be).

While the NDPR (unlike the data protection regime in some other jurisdictions) does not make special provision for the use of CCTV, the installation or use of data captured via CCTV must at least comply with the relevant grounds for lawful processing of personal data under Section 2.2 of the NDPR.

Given that it may not always be practical to obtain consent from the data subject due to the nature of how data is collected by CCTV, the data collector must ensure that any processing of PII data captured or collected by CCTV is done transparently in compliance with Section 3.1(1) of the NDPR. The controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear

and plain language, and for any information relating to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Thus, in our view, it would be best practice to bring the use of CCTV in any specified area to the attention of the data subject and, where necessary, specify the purpose(s) of collection as provided under Section 2.1(1) of the NDPR. This may include the use of a high-visibility sign or any other form of notice that gives the data subject the right to consent (or object) to the collection of his or her personal data through CCTV.

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

Yes, CCTV data can only be processed for the purposes for which consent was granted/obtained and for any other lawful purpose as may be provided by law. For example, CCTV data may be used as computer-generated evidence pursuant to Section 84 of the Evidence Act 2011, or may be used by law enforcement agencies for the purposes of a criminal investigation subject to an order of a court of competent jurisdiction under the Cybercrime Act.

14 Employee Monitoring

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

Employee monitoring is only permitted where the monitoring is done with the consent of the employee (in line with the NDPR) and to the extent that it does not infringe on the employee's right to privacy as guaranteed under Section 37 of the 1999 Constitution.

In terms of monitoring work emails or correspondence, in most cases, the right of the employer to monitor is usually already retained in the terms and conditions of employment. Where this is not the case it is advisable, from an abundance of caution, that the consent of the employee be obtained prior to such monitoring. In the alternative, the company may take steps to ensure that monitoring policies are put in place prior to carrying out any employee monitoring.

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

The informed consent of the employee will be required pursuant to Section 2.2(a) of the NDPR. Employers typically obtain consent from the onset of the employment relationship through the contracts of employment or through some other form of written authorisation or mandate in line with the requirements for valid consent under Section 2.3 of the NDPR.

Section 2.3 states that: (1) no data shall be obtained except where the specific purpose of collection is made known to the data subject; and (2) the data controller is under an obligation to ensure that the consent of a data subject has been obtained without fraud, coercion or undue influence; accordingly: a) where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data and the legal capacity to give consent; b) if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding on the data subject; c) prior to giving consent, the data subject shall be informed of his or her right and method to withdraw his or her consent at any given time. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal; d) when assessing whether consent is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary (or is excessive) for the performance of that contract; and e) where data may be transferred to a third party for any reason whatsoever.

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

The NDPR does not provide for consultation with trade unions for monitoring purposes. The right to data privacy is personal to the data subject; therefore, to the extent that the employee has consented to being monitored, consultation with trade unions or employee representatives will not be necessary unless the contract of employment specifies otherwise.

15 Data Security and Data Breach

15.1 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 a general obligation to ensure the security of personal data under the NDPR.

Section 2.6 of the NDPR provides that anyone involved in data processing or the control of data shall develop security measures, including measures for protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems, and continuous capacity-building for staff.

Based on the foregoing, the obligation to ensure data security is imposed on both data controllers and processors.

In addition, Section 2.4(b) of the NDPR specifies that every data processor or controller shall be liable for the actions or inactions of third parties who handle the personal data of data subjects.

15.2 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.

Para. 12 of the NDPRIF requires data controllers and administrators to report to NITDA any breach within 72 hours of

having knowledge of the breach. The Report is expected to include the number of data likely to be affected, the cause of the breach and remedial actions being taken.

The notification of a data breach to NITDA must include the following information:

i. A description of the circumstances of the loss or unauthorised access or disclosure.
ii. The date or time period during which the loss or unauthorised access or disclosure occurred.
iii. A description of the personal information involved in the loss or unauthorised access or disclosure.
iv. An assessment of the risk of harm to individuals as a result of the loss or unauthorised access or disclosure.
v. An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorised access or disclosure.
vi. A description of any steps the organisation has taken to reduce the risk of harm to individuals.
vii. A description of any steps the organisation has taken to notify individuals of the loss or unauthorised access or disclosure.
viii. The name and contact information for a person who can answer, on behalf of the organisation, the Agency's questions about the loss or unauthorised access or disclosure.

NITDA also recommends that organisations adopt a self-reporting approach by reporting data breaches to NITDA within a reasonable timeframe (no later than 72 hours).

15.3 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.

No. However, please see our response to question 15.2 above regarding the relevant details to be reported.

15.4 What are the maximum penalties for data security breaches?

Section 2.10 of the NDPR provides that, in addition to any other criminal liability, a person found to be in breach of the NDPR shall be liable: (a) in the case of a data controller dealing with more than 10,000 data subjects, to a fine of 2% of the Annual Gross Revenue of the preceding year or payment of the sum of ₦10 million (approx. US$27,000), whichever is greater; and (b) in the case of a data controller dealing with less than 10,000 data subjects, payment of a fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of ₦2 million (approx. US$6,000), whichever is greater.

Further, in the event that the data breach amounts to an offence under the Cybercrime Act, or any other sector-specific legislation, the person in breach may be subject to a term of imprisonment or additional fines or both, depending on the breach and the actions under the relevant laws.

16 Enforcement and Sanctions

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

Investigatory/Enforcement Power	Civil/Administrative Sanction	Criminal Sanction
NITDA Pursuant to Section 1 of the NITDA Act 2007 and Section 4.1 of the NDPR, NITDA is responsible for the enforcement of the NDPR and the NITDA Act. Specifically, Section 4.1 (4) of the NDPR gives NITDA the power to register and license DPCOs who shall, on behalf of the Agency, monitor, audit and conduct training and data protection compliance consulting with all data controllers under the NDPR. Further, Section 4.2 of the NDPR empowers NITDA to set up an Administrative Redress Panel (without prejudice to the right of a data subject to seek redress in a court of competent jurisdiction) that shall be responsible for the investigation of alleged data breaches and, where applicable, determine the appropriate redress.	Under the NDPR, a person found to be in breach of the NDPR shall be liable: (a) in the case of a data controller dealing with more than 10,000 data subjects, to a fine of 2% of the Annual Gross Revenue of the preceding year or payment of the sum of ₦10 million (approx. US$27,000), whichever is greater; and (b) in the case of a data controller dealing with less than 10,000 data subjects, to payment of a fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of ₦2 million (approx. US$6,000), whichever is greater.	Section 17(1) of the NITDA Act 2007 criminalises non-compliance with the provisions of the Act. In this regard, Section 18(1) of the Act provides that a person who commits an offence under this Act where no specific penalty is provided, is liable on conviction: (a) for a first offence, to a fine of ₦200,000.00 (approx. US$600) or imprisonment for a term of one year, or to both such fine and imprisonment; and (b) for a second and subsequent offence, to a fine of ₦500,000.00 (approx. US$1,300) or to imprisonment for a term of three years, or to both such fine and imprisonment.
NCC The NCC established by virtue of the Nigerian Communications Act 2003 is also a data regulator within the telecommunications sector. The NCC derives its investigatory power from Section 61 of the NCC Act, which provides that the NCC may investigate any matter pertaining to the administration of the Act or its subsidiary legislation if the NCC has grounds to believe that an infringement – civil or criminal – of the provisions of this Act or its subsidiary legislation was, is or will be committed.	Section 21 of the RTS Regulations provides that any entity, including licensees, independent registration agents or subscriber registration solution providers, who retains, duplicates or deals with subscribers' information in contravention of any of the provisions of the RTS Regulations, is liable to a penalty of ₦200,000.00 (approx. US$600) per Subscription Medium and, where a subscriber's	By Section 140 of the NCC Act, where no specific penalty is prescribed, or its subsidiary legislation for any offence, a person found guilty of such offence shall be liable: (a) as a first offender, to a fine not exceeding ₦100,000.00 (approx. US$300) or to imprisonment for a term not exceeding one year, or to both such fine and imprisonment; and (b) for a subsequent conviction, to a fine not exceeding ₦500,000.00 or to

Investigatory/Enforcement Power	Civil/ Administrative Sanction	Criminal Sanction
(contd.) By virtue of the NCC Registration of Telephone Subscribers Regulations, 2011 ("RTS Regulations"), all mobile network operators are required to register the mobile phone numbers of all subscribers on their network. As a result, network operators process personal data in this regard. Therefore, non-compliance with the Regulation is a legal basis for the NCC to commence investigation and enforcement. Section 55 of the Consumer Code of Practice Regulations, 2007 ("**Regulation**") also gives the NCC the power to investigate complaints of non-compliance with the Regulation.	*(contd.)* information has been utilised in any business, commercial or other transactions, such entity is liable to a penalty of ₦1 million (approx. US$3,000) per Subscription Medium.	*(contd.)* imprisonment for a term not exceeding three years, or to both such fine and imprisonment.
NIMC The NIMC, by virtue of Section 5 of the NIMC Act 2007, is also a data protection agency with the responsibility to ensure the preservation, protection, sanctity and security (including cybersecurity) of any information or data collected, obtained, maintained or stored in respect of the National Identity Database. Section 28(1) of the NIMC Act provides that any person who (a) without lawful authorisation, accesses data or information contained in the database, (b) refuses to provide relevant data or information to the NIMC, or (c) knowingly or recklessly makes a statement or provides information to the NIMC which is false in any material way, commits an offence.	N/A	In the case of a person, non-compliance with Section 28(1)(a) of the NIMC Act is an offence and shall entail liability, upon conviction, to imprisonment for a term of not less than 10 years without the option of a fine. Whereas, in relation to other provisions of Section 28(1), the person shall be liable, on conviction, to a fine of not less than ₦250,000 (approx. US$750) or an imprisonment term of not less than three years, or both. In the case of a corporate body, a fine of ₦10 million (approx. US$27,000) shall be payable upon conviction in relation to Section 28(1)a, and a fine of ₦1 million (approx. US$3,000) in relation to other provisions of Section 28(1).
CBN The CBN has the overall power within the Nigerian financial services sector to regulate, investigate and subject to the enabling law sanction banks, financial institutions, and any other licensee. **Credit Reporting Act ("CRA") 2017** The CRA provides for the creation of credit bureaux that will be responsible for the receiving, collation and compiling of credit and credit-related information from credit information providers, credit information users and such other persons as the Act may prescribe. Section 8 of the CRA gives the CBN the power to license, regulate, supervise and monitor credit bureaux (including the power to carry out routine examination and investigation). On the basis of the above, credit bureau businesses process data and come under the purview of the CBN. **Bank Verification Number ("BVN") Operations and Watch-list for the Nigerian Banking Industry** The CBN, by virtue of the Regulatory Framework for BVN Operations and Watch-list for the Nigerian Banking Industry ("**BVN Framework**"), is also a data protection agency and reserves the power to impose penalties on organisations for non-compliance with the BVN Framework. The BVN Framework provides for the mandatory capturing of customer data by allocating a Unique ID across the banking industry to each customer of Nigerian banks, and linking such Unique ID to all related bank accounts. Therefore – subject to payment of an access fee and the approval of the CBN – CBN licensees, law enforcement agencies and other entities (as applicable) are granted permission to access BVN information.	N/A	On a combined reading of Section 20(1)(c) and Section 21(2) of the CRA, any person who intentionally or negligently discloses credit information in contravention of the provisions of the CRA commits an offence and is liable, upon conviction, to a fine of not less than ₦10 million (approx. US$27,000). The intentional or negligent provision of inaccurate, misleading or false credit information also attracts a similar penalty. Section 21(4) of the CRA provides that, notwithstanding any provisions of the CRA, the CBN may impose a monetary penalty or even suspend the licence of the credit bureau. Further, the contravention of any provision of the CRA for which no penalty is provided will attract a fine of not less than ₦10 million (approx. US$27,000) or a prison term of 10 years, or both.

Investigatory/Enforcement Power	Civil/ Administrative Sanction	Criminal Sanction
Cybercrime Act Under Section 38 of the Cybercrime Act, service providers are required to maintain all traffic data and subscriber information for a period of two years, and a law enforcement agency may request such data, which shall only be used for legitimate purposes, in line with the Cybercrime Act, any other legislation or an order of court. The Act defines "service provider" as: (i) any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices or mobile networks; and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service (Section 58). Section 39 of the Cybercrimes Act provides for circumstances under which data may be intercepted for the purposes of a criminal investigation or proceedings, subject to obtaining a valid order from a court of competent jurisdiction.	N/A	Section 38(6) of the Cybercrime Act provides that any person who contravenes Section 38 shall be liable, on conviction, to imprisonment for a term of not more than three years or a fine of not more than ₦7 million (approx. US$19,000), or both.

16.2 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?

This will generally depend on the powers of the relevant data protection authority under the enabling law. For example, under Para. 5.1.4 of the NDPRIF, depending on the severity of the breach, NITDA may issue administrative orders, including:

i. Suspension of the service pending further investigations.
ii. For parties in breach to appear before a panel to determine liability of officers.
iii. A public notice to warn the public to desist from patronising or doing business with the affected party.
iv. Referring the parties in breach to another Self-Regulatory Organisation ("**SRO**") for appropriate sanctions.

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

Data protection authorities typically follow due process in investigating breaches, and generally carry out enforcement actions as a last resort, having given the data controller/processor an opportunity to represent itself or provide tenable explanations. For example, the NCC issued the Registration of Telephone Subscribers Regulations in 2011 and gave network operators a number of years to comply. It was not until 2015 that the NCC fined certain telecoms operators in Nigeria for failure to carry out the prescribed subscriber data collation exercise.

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

Yes. However, such enforcement is typically in respect of businesses with some form of legal presence in Nigeria; otherwise, in most instances, it is almost impracticable to commence an enforcement exercise against businesses outside Nigeria. It must, however, be noted that the NCC and the Nigerian Broadcasting Corporation (where applicable) may block online access from Nigerian geolocations to such non-compliant company.

That said, it is useful to note that in order to ensure the enforcement of the NDPR in foreign countries and international organisations, Section 4.3 of the NDPR requires NITDA and relevant authorities to take steps to do the following:

a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance, and information exchange;
c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and
d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

This will generally depend on the nature of the data sought. If the discovery would involve the disclosure of PII of a Nigerian, then such disclosure will be subject to the data subject's consent, since the controller will most likely not be bound or compelled by the laws of the foreign enforcement agencies to disclose the required personal information. Similarly, where it involves classified government-related information, the relevant regulatory approvals must also be sought, and such consent/clearance obtained before disclosure can be made.

Again, depending on the subject matter of the e-discovery, an official mutual legal assistance ("**MLA**") request can be made to the Ministry of Justice, which serves as the central authority in relation to MLA requests. It should, however, be noted that this is subject to the existence of a valid bilateral agreement between the Federal Republic of Nigeria and the country of the law enforcement agency making the request.

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

No specific guidance on e-discovery has been issued by any data protection authority to date.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

On 4 October 2019, NITDA released a statement on the status of its investigation into a potential breach of privacy rights of Nigerians by Truecaller. However, NITDA is yet to commence enforcement actions against Truecaller for this possible breach of the NDPR.

The Minister of Communications and Digital Economy recently directed the NCC to disconnect/block all unregistered telephone lines, as per the RTS Regulation.

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

Below is a non-exhaustive list of some of the topical issues for data protection regulators in Nigeria.

1. **Enforcement Actions**
   Given that the NDPR is fairly recent, there is a dearth of decided cases and enforcement actions on the provisions of the NDPR. Also, regulators are faced with the challenge of how to commence enforcement actions against data processors that have no corporate presence in Nigeria. Practically speaking, it is almost impossible to sanction data processors that have no corporate existence in Nigeria.
2. **The Use of Cryptography and Blockchain**
   The use of cryptography and blockchain as secure techniques of information management is on the rise. On this basis, regulators are constantly engaging stakeholders to use secure techniques to process and store personal data. NITDA issued the Public Key Infrastructure Regulation in 2013 in order to encourage the use of public key infrastructure ("**PKI**")-based digital certificates to protect the integrity of personal data.
3. **Unified Database**
   Data regulators are exploring ways to have a unified database that enables collaboration, such that regulators do not have to maintain separate databanks. For example, the NIMC manages the national identity database, the NCC manages telecommunication subscribers' personal information, while the CBN maintains BVN data.

Emmanuel Ghahabo is a Partner in the TMT, Dispute Resolution, Corporate Governance and Compliance Practices of the firm.
Emmanuel is a specialist in technology, media and telecommunications law. He has extensive experience and provides exceptional legal advice to the world's leading technology companies on diverse issues including: advertising law; data privacy and protection; drafting and negotiation of information technology agreements; e-commerce; cloud computing and adoption; patents, copyright and industrial designs; cybersecurity; fintech regulation and compliance; technology licensing, acquisition, terms of use and franchising; international joint ventures in the telecommunications industry; as well as regulatory and licensing regimes.
He also handles trademarks and other IP-related disputes arising from breach of licensing agreements or general unauthorised usage.
Emmanuel also has nearly three decades of experience both as a seasoned litigator and a trusted compliance and corporate counsel. He is highly regarded for his work in conducting and/or advising on some of the most sensitive corporate internal investigations that have occurred in the Nigerian market in the past 15 years. His practice includes representing corporations, directors and officers, as well as regulatory and public authorities, in connection with white-collar crime, asset tracing, governance and compliance matters.

Templars
5th Floor, 13A, A.J. Marinho Drive
Victoria Island
Lagos
Nigeria

Tel: +234 1 4611 292 94
Email: emmanuel.gbahabo@templars-law.com
URL: www.templars-law.com

Oghomwen Akpaibor is a Senior Associate in the TMT and Corporate and Commercial Practices of the firm. She has over 10 years of legal experience guiding both local and multinational organisations in navigating the intricacies of domestic and international business transactions. Her key areas of specialisation include general corporate advisory, technology, employment, regulatory compliance and intellectual property. As a key member of the corporate team, she regularly advises on legal and regulatory requirements relevant to the establishment and operation of businesses in Nigeria, and has extensive experience in regulatory compliance, labour and employment, corporate restructuring and immigration.
Oghomwen has a deep understanding of the legal, business and technological considerations surrounding technology. Her expertise covers advising on technology-related transactions with the aim of minimising client risks, especially in matters that touch on cybersecurity, e-commerce, fintech and consumer protection, among others.
Oghomwen also regularly advises clients on intellectual property rights, data privacy issues arising from the processing of personal data and cloud computing, licensing requirements and policies, as well as market developments within the highly regulated ICT space.

Templars
5th Floor, 13A, A.J. Marinho Drive
Victoria Island
Lagos
Nigeria

Tel: +234 1 4611 292 93
Email: oghomwen.akpaibor@templars-law.com
URL: www.templars-law.com

Templars is one of the foremost integrated, full-service commercial law firms in Nigeria. With 90+ lawyers and 15 Partners working out of our offices in the key commercial centres (Lagos and Abuja), we are strategically placed to offer quality legal services to clients across the length and breadth of the country.
At Templars, our strengths lie in diverse legal fields as well as in the major sectors of the Nigerian economy. We are well versed in domestic and international business transactions involving strategic alliances and business arrangements, and our lawyers work daily with all types of businesses, large and small, to negotiate, structure and document their transactions. Our lawyers are trained to diagnose and break down business problems from a commercial perspective and don the lawyer's hat to pursue business-savvy legal solutions.

Templars also has a robust TMT Practice. In the technology and telecoms sector, our excellent relationships with various industry regulators and government agencies play a vital role in our capacity to provide well-tailored and exceptional legal advice to our clients in diverse areas of operation.
Consistent with our commercial and proactive approach in the service of our clients, we constantly employ cost-effective procedures in the pursuit of each mandate.

www.templars-law.com

TEMPLARS

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
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
Outsourcing
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
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group