ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

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

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2018

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Nigeria

Jackson, Etti & Edu

Ngozi Aderibigbe

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

There are several legislations that contain data protection provisions; however, the most comprehensive statutory instrument on data protection is a subsidiary legislation made pursuant to the National Information and Technology Development Agency Act, 2007 ("NITDA Act"). The NITDA Act authorises the National Information and Technology Development Agency ("NITDA") to develop guidelines for electronic governance and to monitor the use of electronic data interchange. Pursuant to this statutory mandate, NITDA has developed the 2013 Guidelines for Data Protection ("NITDA Guidelines"). The NITDA Guidelines stand out from other legislations because unlike other legislations that contain data protection provisions merely as ancillary to the legislations' primary objectives, the NITDA Guidelines are principally for the purpose of prescribing guidelines for data protection.

There are views that suggest that the NITDA Guidelines are merely advisory and lack the force of law – these views may have been influenced by the permissive language of the Guidelines. However, it is important to note that, under Nigerian law, subsidiary legislations have the same force of law as their respective principal legislations and are therefore equally binding and enforceable. Therefore, in view of the fact that the NITDA Guidelines are a subsidiary legislation, having been enacted pursuant to the NITDA Act (the principal legislation), we believe that it is correct to find that the NITDA Guidelines have the force of law.

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

As with most jurisdictions, Nigeria's data protection and privacy regime takes its earliest definition from the country's constitution – the 1999 Constitution of the Federal Republic of Nigeria. Section 37 of the Constitution guarantees the protection of the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. This protection is guaranteed as a fundamental right of every Nigerian citizen and is therefore the bedrock of Nigeria's data protection regime.

Besides the NITDA Guidelines, the following legislations also preserve citizens' right to privacy of personal data:

(a) The Freedom of Information Act 2011

The objective of this Act is to make public records and information held by Government agencies more freely accessible by the public. It does, however, create an exception with respect to personal records and information. Section 14 of the Freedom of Information Act restricts Government agencies from disclosing personal information by a public institution unless the individual's consent is obtained, or the information is available to the public.

(b) The Child Rights Act 2003

The purpose of this Act is the protection of the Nigerian child, defined as persons under the age of 18 years. Section 3 of the Act reinforces the constitutional rights of every child as provided under the Constitution, which includes the right to privacy provided under section 37 of the Constitution. More specifically, section 8 of the Act guarantees the child's right to privacy, subject to the parents' or guardians' right to exercise supervision and control the child's conduct.

(c) Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes Act has as its general purpose the prevention and prosecution of cybercrimes. It places a duty on computer and mobile network and communication service providers to retain traffic data and subscriber information for a period of two years. It also requires such service providers to have regard to the individual's right to privacy under the Constitution and to take measures to safeguard the confidentiality of data processing for the purpose of law enforcement.

The Cybercrimes Act also mandates financial institutions to put in place effective measures to safeguard the sensitive data of their customers.

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

The following sector-specific legislations contain certain data protection provisions:

The Telecommunication Sector: The Nigerian Communications Commission Consumer Code of Practice Regulations 2007

The Nigerian Communication Commission ("NCC") is the regulatory body for the telecommunications industry in Nigeria. Pursuant to powers conferred by its enabling Act – the Nigerian Communications Commission Act 2003 ("NCC Act") – the NCC has published the NCC Consumer Code of Practice Regulations 2007 for telecommunication service providers. The Schedule to the NCC Consumer Code of Practice contains the General Consumer Code of Practice. This Code applies only to providers of

communication services in Nigeria. It sets out principles to regulate the collection and maintenance of consumers' personal information and requires such service providers to ensure the protection of such information. The Code further requires telecommunication companies to implement appropriate policy to ensure proper collection, use and protection of consumer information, and to ensure that third parties with whom telecommunication companies transact with have adopted appropriate measures for the protection of consumer information.

The NCC Consumer Code of Practice Regulations 2007 is being revised.

The Telecommunication Sector: Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011

The Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 ("Registration of Telephone Subscribers Regulation") are applicable to telecommunications companies. Regulations 9 and 10 of the Registration of Telephone Subscribers Regulation contain data protection provisions. Regulation 9 guarantees the confidentiality of subscriber information held in the NCC's Central Database. It also recognises the subscriber's right to view and update their personal information held in the NCC's Central Database or the database of any telecommunication company.

The Financial Sector: Central Bank of Nigeria's Consumer Protection Framework 2016

The Central Bank of Nigeria's Consumer Protection Framework 2016 ("CBN Consumer Protection Framework") is a subsidiary legislation made pursuant to the Central Bank of Nigeria Act of 2007. Section 6(2) of this subsidiary legislation imposes a burden on financial institutions to maintain the confidentiality and privacy of all financial services customers – present or past. Appropriate data protection measures and staff training programmes are to be put in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers are also required to obtain the written consent of consumers before their data is shared with third parties or used for promotional offers.

The Financial Sector: Credit Reporting Act of 2017

The Credit Reporting Act of 2017 provides a framework for credit reporting by credit bureaux. Section 5 of the Act requires credit bureaux to maintain credit information for at least six years from the date on which such information was obtained, after which the information should be archived for a further period of 10 years. It may thereafter be destroyed by the credit bureau. Section 9 of the Act reiterates the rights of data subjects (i.e. persons whose credit data are held by a credit bureau) to the privacy, confidentiality and protection of their credit information, and prescribes the preconditions under which data subjects' credit information may be disclosed.

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

There is no designated general regulator for data protection in Nigeria. Thus, the regulators for specific legislations are deemed to have authority to enforce data protection provisions of the respective legislations.

Regulator	Legislation
Nigerian Information Technology Development Agency (NITDA)	■ The NITDA Guidelines for Data Protection 2013
Nigerian Communications Commission (NCC)	■ Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 ■ The NCC Consumer Code of Practice Regulations 2007
Central Bank of Nigeria (CBN)	■ Central Bank of Nigeria's Consumer Protection Framework 2016 ■ Credit Reporting Act of 2017

2 Definitions

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

- **"Personal Data"**

  The NITDA Guidelines define personal data to mean any information relating to an identified or identifiable natural person ("data subject"). It includes information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an e-mail address, bank details, posts on social networking websites, medical information, and other unique identifiers such as, but not limited to, a MAC address, IP address, IMEI number, IMSI number, SIM and others.

  The data protection provisions contained in the Registration of Telephone Subscribers Regulation use the phrase "personal information" which is defined therein as the full names (including mother's maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of subscribers.

- **"Processing"**

  "Processing of Personal Data" is defined under the NITDA Guidelines to mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

- **"Controller"**

  The NITDA Guidelines define "data controller" to mean any person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by an Act of National Assembly or regulations, the controller or the specific criteria for his nomination will be as stated by the Act or regulation.

- **"Processor"**

  This term is not defined in the NITDA Guidelines nor in any other relevant legislation.

- **"Data Subject"**

  Under the NITDA Guidelines, "data subject" means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his 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 and trade-union membership.

- **"Data Breach"**

  This term is not captured in the NITDA Guidelines or any other relevant legislation.

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

  The following definitions are provided in the NITDA Guidelines:

  - "Data Subject's Consent": this means any freely given specific and informed indication of a data subject's wishes by which the data subject signifies his agreement to personal data relating to him being processed.
  - "Personal Data Filing System": means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed.
  - "Data Portability": means the ability for data to be transferred easily from one IT system to another through a safe and secure means in a standard format.

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?

Yes, the NITDA Guidelines extend to organisations outside Nigeria to the extent that such organisations process personal data of Nigerian citizens.

4 Key Principles

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

- **Transparency**

  Where personal data has been obtained otherwise than from the data subject, sections 2.1(3) and 2.2(3) of the NITDA Guidelines place a requirement on the data controller to disclose to the data subject the following information, except where the data subject already has it:

  - the identity of the controller and of the representative, if any;
  - the purpose for which the data is being processed; and
  - any further information, such as the categories of data concerned, the recipients or categories of recipients, the existence of the mechanism for access to, and mechanism for rectifying, the data subject's data.

  In addition, section 2.1(9) of the Guidelines provides that a data subject should be able to obtain from data controllers, without constraint, information on the data subject's personal data being processed, including the category of data, identity of any third-party recipients of the data, the source of the data, the procedure for any automatic processing of data, etc.

  Section 4.1.1 of the NITDA Guidelines also requires data controllers to inform data subjects about the purpose for which the data is being collected. If the data is to be sent outside Nigeria, the data controller is expected to inform the data subjects of this fact.

  The NCC Consumer Code of Practice Regulation 2007 provides that any telecommunication service operator that collects information on individual consumers should have an accessible and easy-to-read policy on the protection of consumer information. The policy should state clearly what information is being collected; the use of that information; possible third-party exchange or disclosure of that information; and the choices available to the consumer regarding collection, use and disclosure of the collected information.

- **Lawful basis for processing**

  Section 2.1(8) of the NITDA Guidelines provides that personal data may be processed only under one of the following conditions:

  - if the data subject has unambiguously given his or her consent to the processing;
  - the processing is necessary in furtherance of a contract to which the data subject is a party;
  - the processing is necessary for compliance with a legal obligation to which the controller is subject to;
  - the processing is necessary to protect the vital interests of the data subject;
  - the processing is necessary in the public interest or in the exercise of the controller's official authority;
  - the processing is required for health management purposes and the data is processed by a health professional who is subject to the obligation of professional secrecy;
  - the processing is in connection with any offences, criminal convictions, etc;
  - the data is processed in connection with administrative sanctions or judgments in civil cases; or
  - the processing is necessary for the purpose of the legitimate interests pursued by the data controller or by the third party or such parties to whom the data is disclosed.

  The NITDA Guidelines provide eight principles for data protection, the first of which is that personal data must be processed fairly and lawfully. The Guidelines require data controllers to inform data subjects about the purposes for which data is being collected. If the data is to be transferred outside of Nigeria, this fact should also be made known to the data subjects.

  The NCC General Consumer Code of Practice Regulations 2007 mandate telecommunication services operators to collect and maintain information on individual consumers in a fair and lawful manner. To this end, telecommunication services operators are required to provide: notice to consumers on the information they collect, and its use or disclosure; the choices consumers have with regard to their personal data; access by consumers to their data; and security measures taken to safeguard consumer's information.

- **Purpose limitation**

  The NITDA Guidelines restrict the use of personal data to the purpose for which the data was collected. Principle 2 stated in section 4.1.2 of the Guidelines requires data controllers to ensure that data collected for one purpose is not used for a different purpose. The purpose for collecting the data must be reasonable and obviously lawful.

  Telecommunication companies are required by the NCC Consumer Code of Practice Regulations to process individual consumers' information for limited and identified purposes. Similarly, Regulation 9 of the NCC (Registration of Telephone Subscribers) Regulations restrains telecommunication companies from using personal information of subscribers in any manner other than for the company's operations and in line with the NCC Consumer Code of Practice.

- **Data minimisation**

  The NITDA Guidelines prevent data controllers from collecting excessive data. Only such data as is necessary, bearing in mind the purpose of the data collection, should be collected by data controllers.

- **Proportionality**

  This term is not captured in the NITDA Guidelines or any other relevant legislation.

- **Retention**

  There is no generally applicable timeline for data retention. The NITDA Guidelines provide that personal data should be kept for no longer than is necessary. It requires data controllers to develop a retention policy for data. A similar provision is contained in the NCC's General Code, which prevents telecommunications companies from keeping information for longer than is necessary.

  The Credit Reporting Act specifically requires credit bureaux to maintain credit information for at least six years from the date on which such information was obtained, after which the information should be archived for a further period of 10 years. It may thereafter be destroyed by the credit bureau.

  Section 38 of the Cybercrimes Act mandates companies that provide communication services or that process or hold computerised data to keep all traffic data and subscriber information for a period of two years.

- *Other key principles – please specify*

  Besides the principles already discussed above, the following Principles are provided for in the NITDA Guidelines:

  (i) Principle 4 – Personal data must be accurate and where necessary kept up to date: This principle requires data controllers to provide data subjects with the option of and a means to update their personal data.

  (ii) Principle 6 – Personal data must be processed in accordance with the rights of the data subject: Data subjects are entitled to request to view their data as held by the data controller, and the data controller is required to respond to such requests without delay.

  (iii) Principle 7 – Appropriate technical and organisational measures must be established to protect the data.

  (iv) Principle 8 – Personal data must not be transferred outside Nigeria unless adequate provisions are in place for its protection in the receiving country.

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**

  Under the NITDA Guidelines, individuals have the right to request for copies of their data which should be made available within seven days of request.

  Section 9(6)(a) of the Credit Reporting Act gives data subjects the right to request for their credit information, which is classified as personal data. Also, under the Registration of Telephone Subscribers Regulation, any telecommunication services subscriber whose personal information is stored by the service provider is entitled to view the said information and to request updates and amendments to the information.

- **Right to rectification of errors**

  Under the NITDA Guidelines, individuals have the right to obtain from the data controller rectification of data not in compliance with the Guidelines. Also, they are entitled to the notifications sent to third parties to whom the data in need of rectification have been disclosed. Principle 4 under the NITDA Guidelines requires that personal data be accurate and kept up to date. Thus, data controllers are expected to provide individuals with the ability to update or correct their personal data as the need arises.

  The Credit Reporting Act, in section 9(6)(b), gives data subjects the right to contest the accuracy of their credit information within 15 days of receiving the credit report, and to have the matter resolved promptly. Also, under the Registration of Telephone Subscribers Regulation, any telecommunication services subscriber whose personal information is stored by the service provider is entitled to request updates and amendments to the information.

- **Right to deletion/right to be forgotten**

  There are no clear provisions on a data subject's right to deletion or right to be forgotten under any of the relevant legislations. However, the NITDA Guidelines provide that data subjects should be able to rectify, erase or block data which does not comply with the provisions of the Guidelines.

- **Right to object to processing**

  The NITDA Guidelines provide that data subjects should have the option to object to and request free of charge the processing of personal data relating to him which the data controller intends to process for the purpose of direct marketing. Individuals have the right to object to processing of data for the purpose of direct marketing and also to object to disclosure of data to a third party.

  The CBN Consumer Protection Framework states that the consent of consumers shall be obtained in writing before their data is shared with third parties, and before using such information for future promotional offers via e-mail, SMS, phone calls and other channels.

- **Right to restrict processing**

  Under the NITDA Guidelines, data subjects should have the option to object to the processing of his or her personal data for the purposes of direct marketing.

- **Right to data portability**

  Under the NITDA Guidelines, a data subject is entitled to obtain from the data controller a copy of his or her personal data in a format usable by the data subject. The data subject is also entitled to request that his or her data be transmitted electronically to another processing system.

- **Right to withdraw consent**

  Under the NITDA Guidelines, individuals are entitled to opt out if data processing is for the purpose of marketing communications.

- **Right to object to marketing**

  The NITDA Guidelines provide that individuals should have the right to object to the processing of data for the purpose of direct marketing or opt out of marketing communications.

- **Right to complain to the relevant data protection authority(ies)**

  The NITDA Guidelines are silent on the individual's right to complain.

  However, the Credit Reporting Act of 2017 provides in Part IV, section 13 that a data subject having complaints regarding the accuracy of the credit information shall submit the complaint in writing to the credit information provider.

- *Other key rights – please specify*

  There are no other specific key rights.

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 NITDA Guidelines do not impose an obligation on a business to register or notify NITDA regarding its data processing activities. Some sector-specific authorities require registration, but this is

mainly to enable the exercise of the Regulator's supervisory role over the regulated entities and not in relation to data processing.

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)?

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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)?

This is not applicable in our jurisdiction.

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)?

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

6.10 Can the registration/notification be completed online?

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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.

The NITDA Guidelines require organisations to appoint Data Security Officers.

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

There are no specific sanctions for failing to appoint a Data Security Officer; however, the general sanction prescribed under the NITDA Act which is applicable to breach of any guidelines made by NITDA (of up to ₦200,000) may be imposed.

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

There is no provision for the immunity of the officer from disciplinary measures in the NITDA Guidelines.

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

The NITDA Guidelines have no express provision as to extent of the Data Security Officer's mandate. However, it does state that organisations shall designate an employee of that organisation as the organisation's Data Security Officer.

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

Being an employee of the subject organisation is the only qualification for a Data Security Officer under the NITDA Guidelines.

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

The Data Security Officer's duties shall include the following:

a. Ensuring that the organisation adheres to the NITDA Guidelines.
b. Ensuring continued adherence to data protection and privacy policies and procedures.
c. Ensuring that personal data is protected and providing for effective oversight of the collection and use of personal information.
d. To be responsible for effective data protection and management within the organisation and ensure compliance with the privacy and data security policies.
e. Providing training and education for employees to promote awareness of and compliance with the privacy and data security policies.

f. Developing recommended practices and procedures to ensure compliance with the privacy and data security policies.

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

There is no requirement for the registration of Data Security Officers in the applicable legislations.

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

There is no obligation to name the Data Security Officer in the organisation's privacy notice.

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?

The NITDA Guidelines require that a data controller who engages the services of another entity to process personal data must have a contract in place with the third-party processor.

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 agreement is required to be in writing and should stipulate that the third-party processor would act only on instructions from the data controller. It should also restrict the data processor from transferring personal data outside Nigeria unless the receiving country ensures an adequate level of protection.

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 NITDA Guidelines require data controllers to pre-notify data subjects before their personal data is used for marketing communications. Data subjects should also have an opt-out option from such communications.

9.2 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.)

In addition to the aforementioned restriction under the NITDA Guidelines, the NCC Consumer Code of Protection restricts telecommunication companies from telemarketing unless they make the following disclosures: the third party on whose behalf it is made and the purpose of the communication; the full price of the product or service which is being marketed; and confirmation that the individual has an absolute right to cancel the agreement for purchase, lease or other supply of any product or service within seven days of the communication, by calling a stated toll-free telephone number. The NCC has also recently mandated all telecommunication service providers to activate a DO-NOT-DISTURB shortcode which allows consumers to opt out of telemarketing communications.

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

There is no specific provision for marketing from other jurisdictions. However, it would appear that marketing from foreign jurisdictions which are delivered to consumers through local telecommunication service providers would be caught by the above provisions of the NCC Consumer Code.

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

The NCC is relatively active in the enforcement of breaches of Consumer Codes. NITDA is however not active in enforcing the NITDA Guidelines.

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

There is no specific provision on purchasing marketing lists. However, the provisions relating to the data subject consents as provided under the NITDA Guidelines and other relevant legislations must be complied with. For example, the NCC Consumer Code of Practice Regulations and the Registration of Telephone Subscribers Regulation prevent telecommunication service providers from granting third-party access to consumers' personal information, except as agreed with the consumer or subject or as provided in the Regulations.

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

There are no specific penalty provisions in the NITDA Guidelines for marketing communications in breach of the Guidelines. However, by section 17(4) of the NITDA Act, where an organisation fails to comply with the guidelines and standards prescribed by NITDA (including the NITDA Guidelines), such organisation commits an offence and may be liable on conviction to a fine of ₦200,000 or imprisonment for a term of one year or both for first time offences; for a second and subsequent offence, to a fine of ₦500,000 or imprisonment for a term of three years or both.

With respect to telecommunication operators, the Nigerian Communications (Enforcement Processes, etc.) Regulations of 2005 have a general provision which penalises telecommunication operators for any breach of any regulations put forth by the NCC. A fine of ₦10,000,000 is the sanction for such breach.

10 Cookies

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

There is no direct legislative restriction on the use of cookies. However, it is relevant to mention that the Cybercrime Act makes it a crime

for a person with intent to defraud to use any device or attachment (including cookies) to obtain information or details of a cardholder.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

11 Restrictions on International Data Transfers

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

The NITDA Guidelines restrict the transfer of personal data outside Nigeria unless adequate provisions are in place for its protection in the receiving country.

11.2 Please describe the mechanisms companies 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 practice, the level of compliance with the provisions of the NITDA Guidelines leaves much to be desired. However, the Guidelines provide that data controllers should consider the following questions in deciding whether personal data should be transferred outside Nigeria:

(a) Does the receiving country have adequate Data Protection Guidelines legislation equivalent to that of Nigeria?

(b) Is it necessary to send the data as part of the fulfilment of a contract?

(c) Has the data subject consented? (Does the fair processing notice include a statement to the effect that it may be transferred outside Nigeria?)

(d) Is the data being processed by another office of the same firm which is established within Nigeria?

(e) Is there a contract in place between the data controller and the receiving organisation providing for adequate protection of personal data?

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.

The NITDA Guidelines do not provide for notification or prior approval for transfer of data outside Nigeria.

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 applicable legislations have no provision on whistle-blowing.

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

This is not applicable in our jurisdiction.

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)?

As part of the application of Principle 1 (personal data must be processed fairly and lawfully), the NITDA Guidelines provide that notices on the purpose and scope of data collection should be displayed prominently where CCTV is used.

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

The applicable legislations have no provision limiting the purpose for which CCTV data may be used.

14 Employee Monitoring

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

There are no specific provisions for employee monitoring. Thus, employee monitoring would be subject to the general provisions on data protection and the individual's rights to privacy.

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

This is not applicable in our jurisdiction.

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

This is not applicable in our jurisdiction.

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.)?

The responsibility to keep personal data secure is placed on the data controller by virtue of the NITDA Guidelines. Under the Registration of Telephone Subscribers Regulation and the Consumer Code of Practice Regulations, the duty to ensure security of personal data is on the telecommunication operator.

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) expects voluntary breach reporting.

The NITDA Guidelines make no provision in this regard.

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) expects voluntary breach reporting.

There are no specific provisions requiring notice of the data breaches to be sent to data subjects.

15.4 What are the maximum penalties for data security breaches?

There is no specific penalty provision in the NITDA Guidelines for breach of data security. However, if such breaches result from noncompliance with any provision of the NITDA Guidelines, then the penalty provisions in the NITDA Act becomes relevant. The NITDA Act provides for liability of up to ₦200,000 or imprisonment for a term of three years or both; such fine and imprisonment for breach of guidelines and standards issued by NITDA.

16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Cybercrimes Act 2015: The Office of the National Security Adviser is to coordinate the administration of the provisions of the Act, while the Attorney General is to ensure effective prosecution of cybercrimes.	No administrative sanctions.	The Act in section 21 provides the sanction for any person who fails to have due regard for an individual's right to privacy and safeguard the confidentiality of the data processed. On conviction, the person shall be liable to imprisonment for a term of not more than three years or a fine of not more than ₦7,000,000, or both.
The NCC Consumer Code of Practice Regulation 2007: Responsible for the enforcement of data protection provisions under this Regulation is the NCC. The NCC's investigatory power includes the conduct of quarterly audits, inspections and monitoring of licensed telecom operators to ensure compliance with its codes and regulations.	This is inclusive of issuance of caution notices to a licensee with no past record, but in the case of continuing breach, the Commission shall determine if they constitute an offence under the NCC Act, including as a breach of applicable licence conditions.	Section 55(3) refers to the Nigerian Communication (Enforcement Processes, etc.) Regulations with respect to penalties for contravening the Code. A fine of ₦10,000,000 is the sanction for such breach.
National Information and Technology Development Agency Act, 2007: The NITDA Act saddles NITDA with the responsibility of investigating and enforcing the provisions of the NITDA Guidelines.	The NITDA Guidelines have no specific applicable administrative or civil sanctions.	A breach of the NITDA Guidelines is a breach of the provisions of the NITDA Act which is an offence under section 17(4) of the NITDA Act. Upon conviction, the individual or body corporate in breach is liable to pay a fine of ₦200,000 or imprisonment for a term of one year, or both, if a first offence. If a subsequent offence, a fine of ₦500,000 or imprisonment of three years, or both.
The Credit Reporting Act of 2017 vests on the Central Bank of Nigeria investigatory power for breaches of the provisions of the Act.	Section 14(e) of the Credit Reporting Act of 2017 states that the Central Bank may revoke a credit bureau's licence if it breaches the provisions of law on data protection.	Section 20(1)(c) of the Act states that a person who intentionally or negligently discloses credit information commits an offence. It is punishable under section 23 with a fine of not less than ₦10,000,000 or imprisonment for a term of 10 years, 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?

The respective regulatory authorities that exercise oversight over legislations with data protection provisions would have power to ban a data processing activity provided that such a ban falls within the statutory powers of the regulatory authority. A court order is not required.

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

The usual approach would be by issuing policies applicable to organisations within the regulator's supervisory control.

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

The respective regulatory authorities may exercise its powers against foreign companies to the extent that the activities of such companies affect the regulated sector. In some cases, regulators may penalise foreign companies by preventing or limiting their continued operation within Nigeria.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

There is no specific rule on how Nigerian companies may respond to foreign e-discovery or disclosure requests.

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

There has been no guidance.

18 Trends and Developments

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

The "enforceability" of the NITDA Guidelines has remained a subject of debate in many circles, largely because of the permissive language predominantly used in the Guidelines. The debate is exacerbated by NITDA's apparent docility in enforcing the provisions of the NITDA Guidelines. There is an increasing call for a full-fledged, principal legislation on data protection to be enacted by the National Assembly and the creation of a Government agency with specific responsibility for data protection. It is believed that having such a primary federal legislation on data protection and a corresponding regulatory agency would significantly strengthen Nigeria's data protection regime.

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

The NITDA Guidelines are currently being updated and reviewed and it is hoped that the updated Guidelines would provide more clarity on the legal status of the Guidelines. NITDA recently confirmed that the reviewed Data Protection Guidelines are currently at the stage of stakeholder consultation.

Ngozi Aderibigbe
Jackson, Etti & Edu
RCO Court
3–5 Sinari Daranijo Street
Victoria Island
Lagos
Nigeria

Tel: *+234 4626 841-3*
Email: *ngoziaderibigbe@jacksonettiandedu.com*
URL: *www.jacksonettiandedu.com*

Ngozi is an intellectual property and commercial law expert. She heads the Technology, Media & Entertainment sector practice at Jackson, Etti & Edu, Nigeria's leading full-service law firm.

Ngozi is involved in providing advice on data protection to local and foreign technology companies. She provides thought leadership on privacy and data protection and its application in today's data-driven business environment.

As a technology savvy lawyer, Ngozi keeps abreast of developments in the technology sector and is knowledgeable about emerging technologies and the applicable legal framework for such technologies. She supports technology companies at every stage of their business cycle – whether as startups or established technology companies. Ngozi also advises on the regulatory framework for companies that create technology, are enabled by technology or whose business model are built around technology.

Jackson, Etti & Edu is a full-service law firm with a sector focus, rendering legal services to Nigerian, Pan-African and International clients in diverse jurisdictions. With over 20 years of valuable experience, our lawyers have gained extensive experience in advising and acting for clients on a wide range of subject matters.

Our firm is recognised for professional legal services of the highest calibre. We draw on our unique knowledge of the African business environment, and in-depth understanding of the economic and socio-political climate in advising clients on a wide range of legal issues.

Sector Focus

One of our key differentiating factors is our strong sector-focused approach. Our key sectors are:

- Energy & Natural Resources.
- Fast Moving Consumer Goods (FMCGs).
- Financial Services.
- Health & Pharmaceuticals.
- Real Estate & Infrastructure.
- Technology, Media & Entertainment.

Our practice areas are:

- Banking & Finance.
- Commercial Intellectual Property.
- Corporate Commercial & General Legal Advisory.
- Litigation & Dispute Resolution.
- Immigration Advisory & Compliance.
- Intellectual Property.
- Real Estate.
- Regulatory & Compliance.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com