Nigeria


Senator Iyere Ihenyen


Rita Anwiri Chindah

Infusion Lawyers

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Nigeria does not have a principal data protection law.

However, Nigeria has subsidiary data protection legislation: the Nigeria Data Protection Regulation 2019 (the Regulation). This Regulation was issued by the National Information Technology Development Agency (NITDA) on 25 January 2019. It is made by virtue of the National Information Technology Development Agency Act (NITDA Act 2007), the principal Act.

By virtue of section 32 of the NITDA Act 2007, NITDA is responsible for making "regulations it deems necessary or expedient for giving full effect to the provisions of the NITDA Act and for effective administration of its provisions". The Regulation repealed the Data Protection Guidelines 2013 ('the Guidelines').

Apart from the Regulation, Nigeria has provisions on data protection in various pieces of legislation and regulations, across a number of industries and sectors.

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

- **The 1999 Constitution of the Federal Republic of Nigeria (as amended)**: The Nigerian Constitution, under section 37, guarantees citizens' privacy as a fundamental human right. It protects citizens' homes, correspondence, telephone conversations, and telegraphic communications. But privacy as a constitutional right may be validly restricted as long as it is "reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom or other persons" (section 45 of the Constitution).
- **The Freedom of Information Act 2011**: The Freedom of Information Act is not a data protection law, but section 14 of the Act protects personal data. Since the Act governs access to public records and information in Nigeria, the section restricts disclosure of personal records without obtaining consent.
- **The Nigerian Communications Act 2003**: By virtue of the powers conferred by the NCA 2003 on the Nigerian Communications Commission (NCC), regulations that touch on data protection in the telecommunications industry have been made by NCC. These regulations are the General Consumer Code of Practice Regulation, the Registration of Telephone Subscribers Regulations ('RTS Regulation') 2011, and the Nigerian Communications (Enforcement Process, etc.) Regulation 2005.
- **The Child Rights Act 2003**: The Act reinforces the constitutional rights of the child, including privacy rights under section 37 of the 1999 Constitution. Under section 8 of the Act, the Nigerian child's right to privacy, family life, home, correspondence, telephone conversation, and telegraphic communications are protected.
- **The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Cybercrimes Act)**: Under the Cybercrimes Act, abuse and misuse of data for fraudulent purposes are criminalised. Service providers have a duty of record retention and data protection. They are to keep all traffic data and subscriber information for a period of two years.
- **The National Identity Management Commission Act 2007 (NIMC Act)**: By virtue of section 31 of the NIMC Act, the National Identity Management Commission (NIMC) makes regulations for the effective operation of the Act. NIMC's powers include the power to provide for the collection, collation, and processing of data and any other relevant information.

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

- **The Consumer Code of Practice Regulations 2007**: In the telecommunications sector, the Code applies to telecom service providers in Nigeria. The Code governs licensed telecommunications operators in Nigeria and related consumer practices.
- **Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 {RTS Regulation}**: Also in the telecommunications sector, it protects data privacy and confidentiality of subscribers' personal data. Collection, collation, management, and storage of subscribers' personal data are regulated.
- **Consumer Protection Framework (the "Framework") 2016**: In the financial sector, the Central Bank of Nigeria (CBN) introduced the Consumer Protection Framework. One of the provisions of this Act is that it protects consumer assets and privacy.
- **The Credit Reporting Act 2017**: In the financial sector, the Credit Reporting Act promotes access to credit information. Amongst other things, it protects the confidentiality rights of data subjects, including the right to consent and the right to accurate personal information.
- **The National Health Act 2014**: In Nigeria's health sector, the National Health Act requires health service providers to keep a record of patients' personal information by storing every user's health records safely and in strict confidentiality.

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

There is no single data protection authority in Nigeria. Under each principal and subsidiary piece of legislation – either general or sector-specific – there are different authorities responsible for data protection:

- **National Information Technology Development Agency (NITDA)**: NITDA issued the Nigeria Data Protection Regulation 2019 and the agency is a data protection authority under the Regulation.
- **Nigerian Communications Commission (NCC)**: NCC is the data protection authority under the General Consumer Code of Practice for Telecommunications, the Registration of Telephone Subscribers Regulation ('RTS Regulation') 2011, the Nigerian Communications' (Enforcement Process, etc.) Regulation 2005, and the Guidelines for the Provision of Internet Service.
- **National Identity Management Commission (NIMC)**: NIMC is the data protection authority under the NIMC Act 2007 and the Mandatory Use of the NIN Regulations 2015 and 2017.
- **Central Bank of Nigeria (CBN)**: CBN is the data protection authority under the Consumer Protection Framework 2016 and the Credit Reporting Act 2017.
- **The Federal Ministry of Health**: The health ministry is the data protection authority under the National Health Act.

2 Definitions

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

- "**Consent**" (of the Data Subject): "any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her".
- "**Data Administrator**": "a person or an organization that processes data".
- "**Data Controller**": "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".
- "**Data Subject**": "any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".
- "**Personal Data**": "any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others".
- "**Personal Data Breach**": "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".
- "**Personal Identifiable Information (PII)**": "information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context".
- "**Processing**": "any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
- "**Sensitive Personal Data**": "data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information".
- "**Third Party**": "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".

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?

Only the Regulation applies to businesses established in other jurisdictions. According to the Regulation, it applies to:

(a) all transactions for the processing of personal data, regardless of the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria; and

(b) all natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria.

4 Key Principles

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

- **Transparency**

  When collecting data, the specific purpose of collection must be made known to the data subject before obtaining consent.

- **Lawful basis for processing**

  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 party or in order to take steps at the request of the data subject before 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 the exercise of an official public mandate vested in the controller.

- **Purpose limitation**

  The Regulation restricts the use of personal data to the purpose for which the data was collected.

- **Data minimisation**

  The Regulation prevents 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**

  The term is not captured in the Data Protection Regulation or any other relevant legislation.

- **Retention**

  There is no general timeline that applies to data retention. The Regulation provides that personal data should be kept for no longer than necessary. It requires data controllers to develop a retention policy for data.

  Similarly, in NCC's General Code of Practice Regulations, telecommunications companies are forbidden from keeping information longer than is necessary.

  The Credit Reporting Act specifically requires the credit bureau 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 businesses 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*

  This is not applicable.

5 Individual Rights

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

Before a data controller may collect the personal data of a data subject, the Regulation requires that the controller informs the data subject of the following rights:

- **Right of access to data or copies of data**

  A data subject has the right to access personal data provided to the controller.

- **Right to rectification of errors**

  A data subject has the right to rectify his or her personal data. This ensures data accuracy.

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

  A data subject has the right to have his or her personal data deleted, erased, or forgotten by the controller, subject to the conditions stated in the Regulation.

- **Right to object to processing**

  A data subject has the right to object to processing. For this purpose, a data subject shall have the option to be expressly and manifestly offered the mechanism for objection to any form of data processing free of charge.

- **Right to restrict processing**

  A data subject has the right to restrict processing of his or her personal data. Once 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 public interest.

- **Right to data portability**

  A data subject has the right to data portability. In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

- **Right to withdraw consent**

  A data subject has the right to be informed by the controller of his or her right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- **Right to object to marketing**

  A data subject has the right to object to the processing of his or her data for marketing. The data subject's personal data shall be safeguarded at all times.

- *Other key rights – please specify*

  Right to structured data: A data subject has the right to receive the personal data which he or she has provided to a controller, in a commonly used structured and machine-readable format.

  Right to make requests to the data controller without charge: A data controller's responses to requests are free of charge as long as the data subject's requests are not manifestly unfounded or excessive.

  Right to make complaint to the Data Protection Authority: This right is to enable a data subject to seek remedy in respect of any alleged breach of his or her data privacy rights whenever an issue arises.

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 Regulation requires that a data controller who processes the personal data of more than 1,000 data subjects in a period of six months must submit a soft copy of the summary of the audit to NITDA.

On an annual basis, a data controller who processes the personal data of more than 2,000 data subjects in a period of 12 months shall, not later than 15 March of the following year, submit a summary of its data protection audit to NITDA.

NITDA is also empowered to register and license Data Protection Compliance Organisations who shall, on behalf of the Agency, monitor, audit, conduct training, and provide data protection compliance consulting to all data controllers under this Regulation.

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)?

The Regulation requires that within six months after the Regulation is issued, each organisation shall conduct a detailed audit of its privacy and data protection practices. The following information must be stated in the audit:

- personally identifiable information the organisation collects on employees of the organisation and members of the public;

- any purpose for which the personally identifiable information is collected;
- any notice given to individuals regarding the collection and use of personal information relating to that individual;
- any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
- 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;
- the policies and practices of the organisation for the security of personally identifiable information;
- the policies and practices of the organisation for the proper use of personally identifiable information;
- organisation policies and procedures for privacy and data protection;
- the policies and procedures of the organisation for monitoring and reporting violations of privacy and data protection policies; and
- 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)?

The basis for registration/notification is per database, specifically where a data controller processes personal data of more than 1,000 data subjects in a period of six months or where a data controller processes personal data of more than 2,000 data subjects in a year.

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)?

Data controllers are required to have Data Protection Officers who will ensure that the data controller adheres to the Regulation, relevant data privacy instruments, and data protection directives of the data controller.

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 answer in 6.2 above.

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

There are no specific sanctions for failing to register/notify NITDA of processing activities. However, by virtue of section 17(4) of the NITDA Act 2007 (the principal Act), a person or body corporate that fails to comply with the guidelines and standards prescribed by NITDA commits an offence. For a first offence, the penalty is a fine of N200,000 (approx. €500) or imprisonment for a term of one year, or both fine and imprisonment. For a second and subsequent offence, the penalty is a fine of N500,000 (approx. €1,240) or imprisonment for a term of three years, or both.

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

No prescribed fee for registration has been specified in the Regulation or made by NITDA.

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

Registration/notification is to be made annually.

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

Apart from the approval of Data Protection Compliance Organisations (DPCOs) through registration and licensing by NITDA, there is no provision for prior approval from NITDA.

6.10 Can the registration/notification be completed online?

This does not apply in our jurisdiction.

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

This does not apply in our jurisdiction.

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

This does not apply 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 appointment of a Data Protection Officer is mandatory.

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

The same penalty stated in question 6.6 above applies.

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?

This does not apply in our jurisdiction.

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

The Regulation does not specify whether a single Data Protection Officer can cover multiple entities.

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

There are no specific qualifications for a Data Protection Officer. What the Regulation requires is that a Data Protection Officer may be outsourced and shall be a "verifiably competent firm or person".

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

The Data Protection Officer's responsibilities as required by law and best practice include the following:

- Ensure that the data controller or processor adheres to the Regulation and relevant data privacy instruments and data protection directives of the data controller.
- Ensure that the data controller or processor has a continuous capacity-building mechanism for his or her own benefit and the generality of the personnel involved in any form of data processing.
- Liaise with regulators in respect of data protection.
- Work with Data Protection Compliance Organisations whose duty it is to provide monitoring, auditing, training, and data protection compliance consulting to data controllers under the Regulation.
- Ensure that the data controller complies with the requirement of periodical data audits, to be submitted to NITDA.
- Ensure that the data controller has policies and procedures for privacy and data protection, including having a publicly available privacy policy.

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

There is no requirement that the appointment of a Data Protection Officer be registered with NITDA or any other relevant authority.

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

There is no express provision for the Data Protection Officer to be named in a public-facing privacy notice. However, the Regulation requires that before collecting personal data from a data subject, the controller must provide the data subject with contact details of the Data Protection Officer.

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. A business that appoints a processor to process personal data on its behalf must have a contract with the 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 Regulation requires that the agreement must be in writing and any person engaging a third party to process the data obtained from data subjects shall ensure adherence to the Regulation.

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 Regulation requires data controllers to pre-notify data subjects before their personal data are used for marketing communications. Section 2.8 of the Regulation also provides data subjects the option to object to the processing of personal data which the data controller intends to process for marketing purposes.

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.).

The Regulation does not restrict electronic marketing, but the NCC Consumer Code of Practice Regulation restricts telemarketing communications. The restriction applies to telecommunication companies. Before a telecommunications company is able to telemarket, it must disclose to the subscriber: (a) the third party on whose behalf the telemarketing communication is made; (b) the purpose of the communication; (c) the full price of the product or service which is being telemarketed; and (d) 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 telemarketing communication via a stated toll-free telephone number. Also, to control telecommunication marketing by enabling subscribers have an opt-out option, NCC introduced a DO-NOT-DISTURB code (2442) in 2016. Once activated, it does not allow a subscriber to receive unsolicited messages from the operators.

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

No. The restrictions do not apply to marketing sent from other jurisdictions, but if the marketing is sent through a local agent or organisation, they may.

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

Of the data protection authorities under the relevant legislation and regulations, NCC has been the most active in enforcing breaches of marketing restrictions.

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

The Regulation is silent about the purchase of marketing lists from third parties, but under the Regulation, any collection or sharing of personal data is subject to the lawful consent of the data subject. Therefore, this requirement to obtain the data subject's consent applies. Also, under the Consumer Code of Practice Regulations and the Registration of Telephone Subscribers Regulation, it is illegal for telecommunication service providers to provide third parties with access to a subscriber's personal data.

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

There are no penalties stipulated under the Regulation, but under the Nigerian Communications (Enforcement Processes, etc.) Regulations of 2005, telecommunication services providers who breach marketing restrictions face a fine of N10,000,000 (approx. €24,380).

10 Cookies

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

The Regulation requires that any medium through which personal data is collected or processed shall display a simple and conspicuous privacy policy which shall, amongst other things, contain technical methods used to collect and store personal information, including cookies, JWT web tokens, etc.

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

This does not apply in our jurisdiction.

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

This does not apply in our jurisdiction.

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

This does not apply in our jurisdiction.

11 Restrictions on International Data Transfers

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

Any transfer of personal data to a foreign country or to an international organisation is subject to the provisions of the Regulation and the supervision of the Attorney General of the Federation. Mainly, it is required that the foreign country has adequate protection for the international transfer of personal data.

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 avoid restrictions on the international transfer of personal data by taking advantage of certain exceptions. These include: (a) obtaining the data subject's explicit and informed consent to the proposed transfer and informing the data subject of possible risks; (b) ensuring that the transfer is necessary for the performance of a contract between the data subject and the controller or to implement precontractual measures; and (c) ensuring that 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.

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.

Yes. The transfer of personal data to other jurisdictions requires the approval of NITDA with the Attorney General of the Federation. This is regardless of the type of transfer. The Attorney General will consider whether the foreign country or international organisation: (a) has adequate protection for data and privacy; (b) has rules and security measures for the transfer of personal data to another foreign country; (c) has effective implementation mechanisms; (d) has independent supervisory authorities to which an international organisation is subject; and (e) is internationally committed, in relation to personal data protection, to legally binding instruments, including multilateral and regional participation.

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.)?

This does not apply in our jurisdiction.

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

This does not apply 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)?

Though the Regulation does not contain provisions for the use of CCTV, it falls under the scope of the Regulation by virtue of section 1.2 of the Regulation. This is because it applies "to all transactions intended for the processing of personal data and to actual processing of personal data *notwithstanding* the means by which the data processing is being conducted or intended to be conducted and in respect of natural persons in Nigeria".

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

This does not apply in our jurisdiction.

14 Employee Monitoring

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

None of the data protection legislation provides for employee monitoring, but employees in Nigeria or of Nigerian descent are data subjects under the Regulation; thus data processing principles and data subject rights apply.

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

The general provision on obtaining the data subject's lawful consent under the Regulation applies.

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

This does not apply 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.)?

Yes. There is a general obligation to ensure the security of personal data. The Regulation requires that anyone involved in data processing or the control of data must have security measures to protect such data.

Both data controllers and processors are responsible for ensuring that security measures are put in place to safeguard personal data. These security measures include protecting systems from hackers, setting up firewalls, storing data securely and ensuring authorised access only, encrypting data, developing organisational policy for handling personal data (and other sensitive or confidential data), ensuring emailing systems' protection, and continuous capacity-building for staff.

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.

No. There is no legal requirement to report data breaches to data protection authorities.

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. There is no legal requirement to report data breaches to data subjects.

15.4 What are the maximum penalties for data security breaches?

In addition to any other criminal liability, the following penalties apply to data breaches under the Regulation:

(a) in the case of a data controller dealing with more than 10,000 data subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of N10 million (approx. €24,800), whichever is greater; and

(b) in the case of a data controller dealing with less than 10,000 data subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of N2 million (approx. €4,900), whichever is greater.

16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
■ NITDA is entitled to receive submissions of copies of the summary of conducted audits from data controllers, which aids its investigatory powers for the purpose of identifying real or potential data breaches under the Regulation. ■ NITDA registers and licenses Data Protection Compliance Organisations who audit and monitor the data protection policies of data controllers and also train data controllers on data protection on NITDA's behalf. ■ NITDA is charged with the duty of setting up the Administrative Redress Panel, whose duty it is to carry out the following functions: (1) investigating allegations of any breach of the provisions of this Regulation; (2) inviting any party to respond to allegations made against it within seven days; (3) issuing administrative orders to protect the subject matter of the allegation pending the outcome of investigation; (4) concluding the investigation and determining the appropriate redress within 28 working days.	■ Not applicable.	■ By virtue of section 17(4) of the NITDA Act 2007, the penalty for breach of the provisions of the Regulations is a fine of N200,000 (approx. €500) or imprisonment for a term of one year for a first offence. For a second or subsequent offence, the civil/administrative sanction is a fine of N500,000 (approx. €1,240) or imprisonment for a term of three years. ■ Where the data controller is dealing with more than 10,000 data subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of N10 million (approx. €24,800), whichever is greater. ■ Where a data controller is dealing with less than 10,000 data subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of N2 million (approx. €4,900), whichever is greater.
■ CBN conducts investigations when necessary, and its findings form the basis for management decisions. ■ CBN reviews, monitors and supervises the operations of credit bureaux under the Credit Reporting Act, and imposes pecuniary and other penalties for the contravention of the Credit Reporting Act. ■ Under the Consumer Protection Framework, CBN employs supervisory mechanisms to effectively enforce consumer protection regulations in the financial services industry.	■ Imposes civil/administrative sanctions such as refunds, suspension from inter-bank activities, denial of approvals, publication of infractions and sanctions, monetary penalties, product recall, suspension/removal of Board/management staff/employees, referral to law enforcement agencies for prosecution, revocation of banking licence, etc. ■ In section 14(e), CBN may revoke the licence of a credit bureau due to a data breach.	■ Under section 20(1)(c) of the Credit Reporting Act, any person who intentionally or negligently discloses credit information in contravention of the provisions of the Act commits an offence punishable under section 23 of the Act. Upon conviction, a minimum fine of N10 million (approx. €23,000) or a 10-year imprisonment applies, or both. The same punishment applies to any person who intentionally or wilfully obtains information from a credit bureau under false pretence or for a purpose other than a permissible purpose.
■ NCC administers the Consumer Code of Practice Regulations and oversees compliance by licensees. Section 55 of the Regulations gives NCC the authority to investigate complaints in the event of any breach of the Code. ■ NCC monitors compliance and imposes penalties in the event of any breaches. It administers the Registration of Telephone Subscribers Regulation 2011 (RTS Regulations). Section 21 penalises entities that retain, duplicate, or deal with subscribers' information in a manner which contravenes the Regulations. ■ NCC enforces the Consumer Code of Practice Regulations and the RTS Registration by virtue of the Nigerian Communications (Enforcement Process, etc.) Regulation 2005.	■ Not applicable.	■ For any violation of the Regulations, the fine is N5 million (approx. €12,350) and a further N500,000 (approx. €1,350) per day for as long as the contravention persists after NCC's notice expires. ■ For violating section 21 of the RTS Regulations, the sanction is N200,000 (approx. €500) per subscription medium. If the entity uses subscribers' information in any business, commercial, or other transactions inconsistent with the Regulations, the entity is liable to a penalty of N1 million (approx. €2,500) per subscription medium.
■ NIMC, as the data protection authority in the national identity management sector, ensures the protection and security (including cybersecurity) of any data collected, stored, or maintained in respect of the National Identity Database. Under section 28(1) of the NIMC Act, it is an offence for a person to: access data or information contained in the database; refuse to provide relevant data or information to the Commission; or knowingly or recklessly provide false information to the Commission.	■ Not applicable.	■ Imprisonment for a term of not less than 10 years without option of fine. Bodies corporate are liable to a N10 million (approx. €23,000) fine.

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
■ Relevant Law Enforcement Agencies ■ Under the Cybercrimes Act, a law enforcement agency may request a service provider to keep any traffic data, subscriber information, and content or non-content information or release any information it has stored. This must be for law-enforcement purposes only. ■ For the purpose of criminal investigations or proceedings, law-enforcement agencies are permitted to intercept electronic communication, subject to obtaining a court order.	■ Not applicable.	■ It is an offence for a service provider to fail to keep any traffic data, subscriber information, and content or non-content information, or to refuse to release to law enforcement agencies or by order of court any information it has stored. Upon conviction, the punishment is imprisonment for a term of not more than three years or a fine of not more than NGN 7 million (approx. €17,300), or both fine and imprisonment. ■ It is an offence for a service provider to refuse to assist a law enforcement agency to intercept electronic communication. Upon conviction, the service provider is liable to a fine of not less than N10 million (approx. €23,000). Each director, manager, or officer of the service provider will also be liable on conviction to not more than three years' imprisonment or a N7 million fine (approx. €17,300), or to both fine and imprisonment.

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?

To the extent that a data protection authority's decision to ban a particular processing activity is within its powers under the relevant legislation, a data protection authority may issue a ban. Therefore, recourse to a court is not required.

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

The data protection authorities tend to give businesses adequate time before taking any enforcement actions. For instance, NCC recently handed down a $5.2 billion fine against MTN after MTN failed to disconnect Subscribers Identification Modules (SIM) with improper registration. MTN had up to 5.2 million unregistered customer lines. MTN was fined $1,000 for each unregistered SIM, amounting to $5.2 billion.

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

A data protection authority may exercise its powers against businesses established in other jurisdictions, as long as those businesses control or process the data of natural persons in Nigeria or residing outside Nigeria who are citizens of Nigeria.

For enforcement, NITDA and the relevant authorities (who are data protection authorities under the relevant legislation) are required to take appropriate steps to develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data through notification, complaint referral, investigative assistance, and information exchange; international mutual assistance is expected in the enforcement of data protection legislation internationally.

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?

There is no standard response for responding to foreign e-discovery requests.

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

No guidance has been issued in our jurisdiction.

18 Trends and Developments

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

The Regulation, issued by NITDA on 25 January 2019, is relatively new. Enforcement trends are yet to emerge. But NCC's $5.2 billion fine against MTN in October 2015 by virtue of NCC's powers under section 20(1) of the Registration of Telephone Subscribers Regulations (TSR) 2011 is one decision that data controllers and processors cannot afford to ignore.

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

Before the new Regulation was made, there were concerns from various quarters about the enforceability of the provisions of NITDA's Data Protection Guidelines 2013, which have been effectively repealed. With the scope of the new Regulation applying to personal data of natural persons in Nigeria and Nigerians outside the country, the "hot topic" is whether relevant data protection authorities in Nigeria have the powers and the enforcement mechanisms to ensure compliance by international organisations. Whether this regulation will also spur data protection authorities to step up their game against local data controllers or processors who violate the privacy of data subjects in various industries and sectors, remains to be seen.

Senator Iyere Ihenyen

Infusion Lawyers
Plot 23, Water Corporation Drive
Victoria Island
Lagos
Nigeria

Tel: +234 809 876 4066
Email: senator@infusionlawyers.com
URL: www.infusionlawyers.com

Senator Iyere Ihenyen specialises in information technology and intellectual property law. He is a thought leader in both areas.

A *DataGuidance by OneTrust* expert on data protection and privacy for Nigeria, Senator advises local and foreign clients on data protection and privacy.

Tech-savvy, Senator works with innovators in the technology space, from intellectual-property-driven innovations to disruptive decentralised ledger technology-powered innovations. He advises and consults for a number of players in the technology space, including Kurecoin and Kurepay, Paxful, and SUREBANQA. Following his work in the space, Senator is Vice Chairman (Policy & Regulations) of the Stakeholders in Blockchain Technology Association of Nigeria (SiBAN) and a Trustee of the African ICT Foundation.

He is a member of the Information & Communications Technology; Intellectual Property; and Sports, Entertainment & Media Committees of the Nigerian Bar Association's Section on Business Law.

Senator is the Lead Partner at Infusion Lawyers. He heads the Intellectual Property & Information Technology team.

Rita Anwiri Chindah

Infusion Lawyers
Plot 23, Water Corporation Drive
Victoria Island
Lagos
Nigeria

Tel: +234 805 629 5765
Email: rita@infusionlawyers.com
URL: www.infusionlawyers.com

Rita Anwiri Chindah, ACIArb specialises in intellectual property, information technology, and Arbitration and Alternative Dispute Resolution (ADR).

A Master's degree holder in Intellectual Property & Information Technology from the University of Derby, UK, Rita is knowledgeable in data protection and privacy, media law, copyright, industrial designs, trademarks, and patents.

Rita has some experience advising startups and companies on intellectual property and technology in the digital age. She also brings her knowledge in Arbitration and ADR to bear, helping clients proactively minimise risks.

Rita is a member of: the Nigerian Bar Association (NBA) Section on Business Law, within the Committees on Arbitration and Alternative Dispute Resolution and Information and Communications Technology; the Chartered Institute of Arbitrators (UK), Nigeria Branch; and the Nigerian Institute of Management.

Rita heads the IP & IT Advocacy team at Infusion Lawyers.

Infusion Lawyers
Your Partner in Innovation

Infusion Lawyers is a virtual intellectual property (IP) & information technology (IT) law firm for the knowledge economy and the digital age.

With its information technology and digital law practices, Infusion Lawyers is on hand to help clients – agencies, established companies, and startups – get data protection and privacy right. In a data-driven global economy, clients need legal and regulatory guide on data protection and privacy. By understanding the risks clients face, we are able to guide clients not only safely but also profitably, maximising safeguards for organisational, corporate, or business growth.

Practice Areas

- Consumer Protection & Competition Law.
- Cybersecurity.
- Digital Law Practice.
- Intellectual Property (IP).
- Information Technology (IT).
- IP & IT Transactional Practice.
- IP & IT Dispute Resolution.
- Regulatory & Compliance.
- Startup Law.
- "Glocal" Practice.

Sector Focus

- Agritech.
- Blockchain & Cryptocurrency.
- Edutech.
- eSports, Betting & Gaming.
- Fast Moving Consumer Goods (FMCGs).
- Fintech.
- Healthtech.
- Technology, Media & Entertainment.