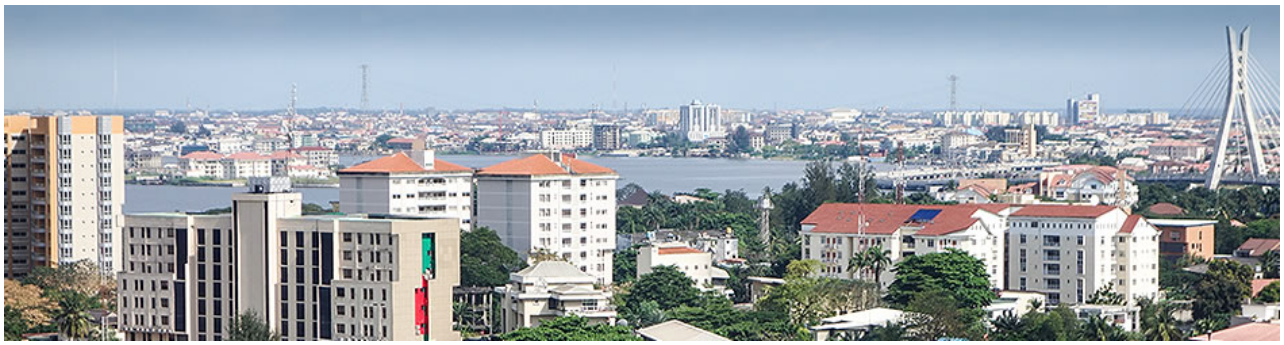
DATA PROTECTION LAWS OF THE WORLD

Nigeria

NIGERIA



Last modified 12 December 2021

LAW

National Information Technology Development Agency (NITDA) issued the Nigeria Data Protection Regulation (NDPR) in 2019.It is the principal regulation and framework for data protection in Nigeria.

The NITDA also issued an Implementation Framework in 2020 in respect of the NDPR and Guidelines for the Management of Personal Data by Public Institutions in Nigeria to regulate personal data processing within public institutions.

Nigeria Data Protection Regulation

The NDPR is the first regulation of its kind governing the use of personal data in Nigeria. The personal and territorial scope of the NDPR is defined by citizenship and physical presence. It applies to residents of Nigeria, as well as Nigerian citizens abroad. The NDPR provides legal safeguards for the processing of personal data. Under the NDPR, personal data must be processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject.

Implementation Framework for the Nigeria Data Protection Regulation

The Framework builds on the NDPR to ensure a tailored implementation of the data protection regime in Nigeria. It serves as a guide to data controllers and administrators/processors to understand the standards required for compliance within their organisations. The Framework is to be read in conjunction with the NDPR and does not supersede the NDPR.

Guidelines for the Management of Personal Data by Public Institutions in Nigeria

In 2020, NITDA issued the Guidelines for the Management of Personal Data by Public Institutions in Nigeria (the Guidelines) to regulate personal data processing within public institutions. The Guidelines apply to all public institutions (PIs) in Nigeria, including Ministries, Departments, Agencies, Institutions, Public Corporations, publicly funded ventures, and incorporated entities with government shareholding, either at the Federal, State or Local levels, that process the personal data of a data subject. The Guidelines mandate all PIs to protect personal data in any incidence of processing of such data. Processing in this context retains the same meaning it has under the NDPR. All forms of personal data of a Nigerian citizen, resident or non-Nigerian individual that has interactions with PIs, or personal data PIs have access to in furtherance of a statutory or administrative purpose, are to be protected in accordance with the NDPR or any other law or regulation in force in Nigeria.

Sectoral Laws

In addition to the principal legislation mentioned, the Constitution of the Federal Republic of Nigeria and various sector-specific laws make different provisions for privacy and data protection matters. These laws are examined below.

The laws

Constitution of the Federal Republic of Nigeria 1999 (As Amended)

The Nigerian Constitution provides Nigerian citizens with a fundamental right to privacy. Section 37 of the Constitution guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. The Constitution does not define the scope of "privacy" or contain detailed privacy provisions.

Child Rights Act 2003

The Child Rights Act 2003 reiterates the constitutional right to privacy as relates to children. Section 8 of the Act guarantees a child's right to privacy subject to parent or guardian rights to exercise supervision and control of their child's conduct. Some Nigerian states have also enacted Child Rights Laws.

Consumer Code of Practice Regulations 2007 (NCC Regulations)

The Nigerian Communications Commission (NCC) issued the NCC Regulations which requires all licensees to take reasonable steps to protect customer information against improper or accidental disclosure, and ensure that such information is securely stored and not kept longer than necessary. The NCC Regulations further prohibit the transfer of customer information to any party except to the extent agreed with the customer, as permitted or required by the NCC or other applicable laws or regulations.

Consumer Protection Framework 2016 (Framework)

The Consumer Protection Framework 2016 was enacted pursuant to the Central Bank of Nigeria Act 2007. The Framework includes provisions that prohibit financial institutions from disclosing customers personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorized access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

Credit Reporting Act 2017

The Credit Reporting Act establishes a legal and regulatory framework for credit reporting by Credit Bureaus. Section 5 of the Credit Reporting Act requires Credit Bureaus to maintain credit information for at least 6 years from the date that such information is obtained, after which the information must be archived for a 10-year period prior to its destruction. Section 9 of the Credit Reporting Act provides the rights of data subjects (i.e. persons whose credit data are held by a Credit Bureau) to privacy, confidentiality and protection of their credit information. Section 9 further prescribes conditions under which the credit information of the data subject may be disclosed.

Cybercrimes (Prohibition, Prevention Etc) Act 2015

The Cybercrimes (Prohibition, Prevention Etc) Act provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. The Act requires financial institutions to retain and protect data and criminalizes the interception of electronic communications.

Freedom of Information Act, 2011 (FOI Act)

The FOI Act seeks to protect personal privacy. Section 14 of the FOI Act provides that a public institution is obliged to deny an application for information that contains personal information unless the individual involved consents to the disclosure, or where such information is publicly available. Section 16 of the FOI Act provides that a public institution may deny an application for disclosure of information that is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege, health workers-client privilege, etc.).

National Identity Management Commission (NIMC) Act 2007

The NIMC Act creates the National Identity Management Commission (NIMC) to establish and manage a National Identity Management System (NIMS). The NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers to qualified citizens and legal residents. Section 26 of the

NIMC Act provides that no person or corporate body shall have access to data or information in the Database with respect to a registered individual without authorization from the NIMC. The NIMC is empowered to provide a third party with information recorded in an individual's Database entry without the individual's consent, provided it is in the interest of National Security.

National Health Act 2014 (NHA)

The NH Act provides rights and obligations for health users and healthcare personnel. Under the NH Act, health establishments are required to maintain health records for every user of health services and maintain the confidentiality of such records. The NH Act further imposes restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information. The NH Act applies to all information relating to patient health status, treatment, admittance into a health establishment, and further applies to DNA samples collected by a health establishment.

Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011

Section 9 and 10 of the Nigerian Communications Commission Regulation provides confidentiality for telephone subscriber records maintained in the NCC's central database. The Regulation further provides telephone subscribers with a right to view and update personal information held in the NCC's central database of a telecommunication company in camera.

The Data Protection Bills

Data protection/privacy is not listed as an item under any of the exclusive, concurrent or residual legislative lists provided in the Nigerian Constitution (as amended). The implication of this is that both Federal and State legislature can legislate on data protection within the country. Pursuant to this, a Federal Data Protection Bill was issued in 2019. The main objective of the Bill is to provide a structure for the protection of personal data and to regulate the processing of information relating to all individuals, irrespective of their nationality. It also seeks to protect the fundamental rights to privacy and freedoms as enshrined in the constitution. However, the status of this Bill is currently unknown as the Federal Ministry of Communications and Digital Economy recently published a request for expression of interest inviting interested law firms and data protection practitioners to submit proposals in respect of drafting a comprehensive data protection law for the Country.

In addition to the above, one state that has considered issuing its own data protection legislation is Lagos State. A data protection bill has been issued by the State House of Assembly and the primary objective of the bill is to promote the protection of personal information processed by public and private bodies in Lagos State and establish minimum requirements for the processing and protection of personal information within the state. The Lagos State Bill has passed second reading and is currently at the House Committee stage. There have been deliberations on the provisions of the bill and stakeholders have proposed changes to its provisions. The eventual state, shape and form of the different laws, if passed remains to be seen.

DEFINITIONS

Definition of personal data

Personal Data is defined as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data is a broad term, encompassing anything from a name, address, photo, email address, bank details, social networking website posts, medical information, and other unique identifier such as, but not limited to, MAC address, IP address, IMEI number, IMSI number, SIM and others.

Definition of sensitive personal data

Sensitive Personal Data means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.

Definition of data subject

Data Subject means an identifiable natural person. An identifiable natural person is 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.

Definition of data controller

Data Controller means a person who either alone, jointly or in common with other persons, or as a statutory body, determines the purposes for and manner in which Personal Data is processed or is to be processed.

Definition of personal data breach

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Definition of processing

Processing means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

NATIONAL DATA PROTECTION AUTHORITY

The National Information Technology Development Agency (NITDA) is currently the main regulator where data protection is concerned in Nigeria. However, sector specific regulatory agencies including Nigerian Communications Commission and the Central Bank of Nigeria provide services relating to the protection of data.

REGISTRATION

There is no requirement to register databases.

DATA PROTECTION OFFICERS

The NDPR requires Data Controllers to designate a Data Protection Officer responsible for ensuring compliance with the NDPR and other applicable data protection directives. The data controller may outsource this responsibility to a verifiably competent firm or person.

COLLECTION & PROCESSING

COLLECTION

Personal Data must be collected and processed in accordance with a specific, legitimate and lawful purpose consented to by the Data Subject.

- Prior to Personal Data collection, Controllers must provide Data Subjects with relevant information, including the identity and contact details of the Controller, contact details of its Data Protection Officer and the intended purpose and legal basis for Personal Data processing.
- The legitimate interests pursued by the Controller or third party must be stated.
    - The recipients or categories of recipients of the Personal Data, if any.
    - Where applicable, the fact that the Controller intends to transfer Personal Data to a third country or international organization, and the existence or absence of an adequacy decision by the Agency, the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.
- Data subjects must be provided with notice of their right to (a) request access to and rectification of Personal Data maintained by the Controller, (b) withdraw consent for further processing by the Controller at any time, and (c) lodge a complaint with the relevant authority.

- Where the Controller intends to process Personal Data for a purpose other than for which it was collected, the controller must provide Data Subjects with any relevant information on the additional purpose prior to further processing.

PROCESSING

Personal Data Processing is lawful if at least one of the following applies:

- The data subject has given consent to the processing of his or her Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller.
- Data processing by a third party shall be governed by a written contract between the third party and the Data Controller. Accordingly, any person engaging a third party to process the data obtained from Data Subjects shall ensure compliance with the NDPR.

TRANSFER

The NDPR includes provisions on Personal Data transfers to foreign countries and international organizations, provided such transfers are intended for processing purposes. The Honorable Attorney General of the Federation (HAGF) is responsible for supervising such Personal Data transfers.

Personal Data transfers are permitted where NITDA determines that a foreign country, territory or specific sector(s) within a foreign country or international organization provide adequate levels of Personal Data protection. The determination is based on the HAGF's consideration of the foreign country's legal system, rule of law, respect for human rights and fundamental freedoms, as well as relevant general and sector-specific legislation in public security, defense, national security and criminal law.

Personal Data transfers may take place without NITDA or HAGF authorization if:

- Data Subject expressly consents to the proposed transfer after being informed of associated risks in the absence of an adequacy determination, the lack of appropriate safeguards, and that there are no alternatives.
- Transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request.
- Transfer is necessary for the performance of a contract in the interests of the Data Subject between the Controller and another natural or legal person.
- Transfer is necessary for important reasons of public interest.
- Transfer is necessary for the establishment, exercise or defense of legal claims.
- Transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Where Personal Data is transferred to a foreign country or to an international organization, the Data Subject shall have the right to be informed of the appropriate safeguards for data protection in the foreign country.

SECURITY

Anyone involved in data processing or the control of data has the responsibility to develop security measures to protect data. Such measures include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policies for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the authorities or to data subjects under the NDPR. However, the Framework mandates Data Controllers to notify NITDA of Personal Data breaches within 72 (seventy-two) hours of becoming aware of the breach. Under the Framework, a Data Controller is also required to immediately notify a Data Subject of a Personal Data breach where the breach will likely result in high risks to the freedoms and rights of the data subject.

ENFORCEMENT

NITDA is empowered to register and license Data Protection Compliance Organizations (DPCOs). On behalf of NITDA, DPCOs monitor, audit, conduct training and data protection compliance consulting to all Data Controllers as defined in the NDPR.

Since the issuance of the NDPR, NITDA has been handed supervisory and enforcement responsibilities in respect of data protection matters in Nigeria. It collaborates with security agencies such as the office of the Inspector General of Police to ensure full compliance and enforcement. Where NITDA has determined that a party is in breach of the NDPR, especially where such breach affects national security, sovereignty and cohesion, it may seek to prosecute officers of the organization as provided for in section 17(1) and (3) of the NITDA Act 2007. To do this, NITDA must seek a fiat of the Attorney General of the Federation or may file a petition with any authority in Nigeria. This may include: The Economic and Financial Crimes Commission, Department of State Security, Nigerian Police Force, Independent Corrupt Practices (and other related offences) Commission or the Office of National Security Adviser. NITDA has also set up an administrative redress panel to (a) investigate allegations of any breach of the provisions of the Regulation (b) invite any party to respond to allegations made against it within seven days (c) issue administrative orders to protect the subject matter of the allegation pending the outcome of investigation and conclude investigations and determine of appropriate redress within 28 working days. A breach of the NDPR is construed as a breach of the NITDA Act 2007. Any organization/entity that contravenes any of the provisions of the NDPR would be in breach and be liable to such fines, sanctions or penalties as may be determined by the Commission from time to time.

Organizations that are in breach of the NDPR requirements can face penalties that vary in amount depending on the number of data subjects affected, as follows:

- if the data breach impacted more than 10,000 data subjects, the organization can be fined up to 2% of its annual revenue or 10 million Naira, whichever is greater;
- if the data breach impacted less than 10,000 data subjects, the organization can be fined up to 1% of its annual revenue or 2 million Naira, whichever is greater.

ELECTRONIC MARKETING

The NCC Regulations provide that no licensee shall engage in unsolicited telemarketing unless it discloses:

- At the beginning of the communication, the identity of the licensee or other person on whose behalf it is made and the precise purpose of the communication
- During the communication, the full price of any product or service that is the subject of the communication
- That the person receiving the communication shall have an absolute right to cancel the agreement for purchase, lease or other supply of any product or service within seven (7) days of the communication, by calling a specific telephone number (without any charge, and that the Licensee shall specifically identify during the communication) unless the product or service has by that time been supplied to and used by the person receiving the communication

Licensees are required to conduct telemarketing in accordance with any "call" or "do not call' preferences recorded by the consumer, at the time of entering into a contract for services or after, and in accordance with any other rules or guidelines issued by the Commission or any other competent authority.

Internet Service Providers (ISP)

The NCC Legal Guidelines for Internet Service Providers (ISP) provides that Commercial Communications ISPs must take reasonable steps to promote compliance with the following requirements for commercial email or other commercial communications transmitted using the ISP's services:

- The communication must be clearly identified as a commercial communication.

- The person or entity on whose behalf the communication is being sent must be clearly identified.
- The conditions to be fulfilled in order to qualify for any promotional offers, including discounts, rebates or gifts, must be clearly stated.
- Promotional contests or games must be identified as such, and the rules and conditions to participate must be clearly stated.
- Persons transmitting unsolicited commercial communications must take account of any written requests from recipients to be removed from mailing lists, including by means of public "opt-out registers" in which people who wish to avoid unsolicited commercial communications are identified.

Advertising

The Nigerian Code of Advertising Practice Sales Promotion and other rights and restrictions on practice provide that all advertisements and marketing communications directed at the Nigerian market using the Internet or other electronic media must comply with the following requirements:

- The commercial nature of such communications must not be concealed or misleading, it should be made clear in the subject header.
- Terms of the offer should be clear and devices should not be used to conceal or obscure any material factors, such as price or other sales conditions likely to influence customer decisions.
- The procedure for concluding a contract should be clear.
- Due recognition must be given to the standards of acceptable commercial behavior held by public groups before posting marketing communications to such groups using electronic media.
- Unsolicited messages should not be sent except where there are reasonable grounds to believe that consumers who receive such communications are interested in the subject matter or offer.
- All marketing communications sent via electronic media should include a clear and transparent mechanism enabling consumers to expressly opt-out from future solicitations.
- Care should be taken to ensure that neither the marketing communication, or applications used to enable consumers to open marketing or advertising messages, interfere with consumers normal use of electronic media.
- Customer information must not be transferred to any party except to the extent agreed with the Customer, as permitted or required by the NCC or other applicable laws or regulations.

ONLINE PRIVACY

The Constitutional right to privacy applies to electronic media, including mobile devices and the Internet. Violations of these rights may be subject to civil enforcement.

The NDPR requires all mediums through which Personal Data is collected or processed to display a simple and conspicuous privacy policy, easily understood by the targeted Data Subject class. The privacy policy must contain the following, in addition to any other relevant information:

- What constitutes Data Subject consent
- Description of Personal Data to be collected
- Purpose of Personal Data collection
- Technical methods used to collect and store personal information (i.e. cookies, web tokens, etc.)
- Access (if any) of third parties to Personal Data and purpose of access
- An overview of data processing principles under the NDPR
- Available remedies for privacy policy violations
- Timeframes associated with available remedies
- Any limitation clause, provided that no limitation clause shall avail any Data Controller who acts in breach of the principles of lawful processing set out in the NDPR.

KEY CONTACTS

Olajide Oyewole LLP
www.olajideoyewole.com/

Sandra Oyewole
Partner
Olajide Oyewole LLP
T +234 1 279 3674
soyewole@olajideoyewole.com

Adewumi Salami
Associate
Olajide Oyewole LLP
T +234 1 279 3674
asalami@olajideoyewole.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.