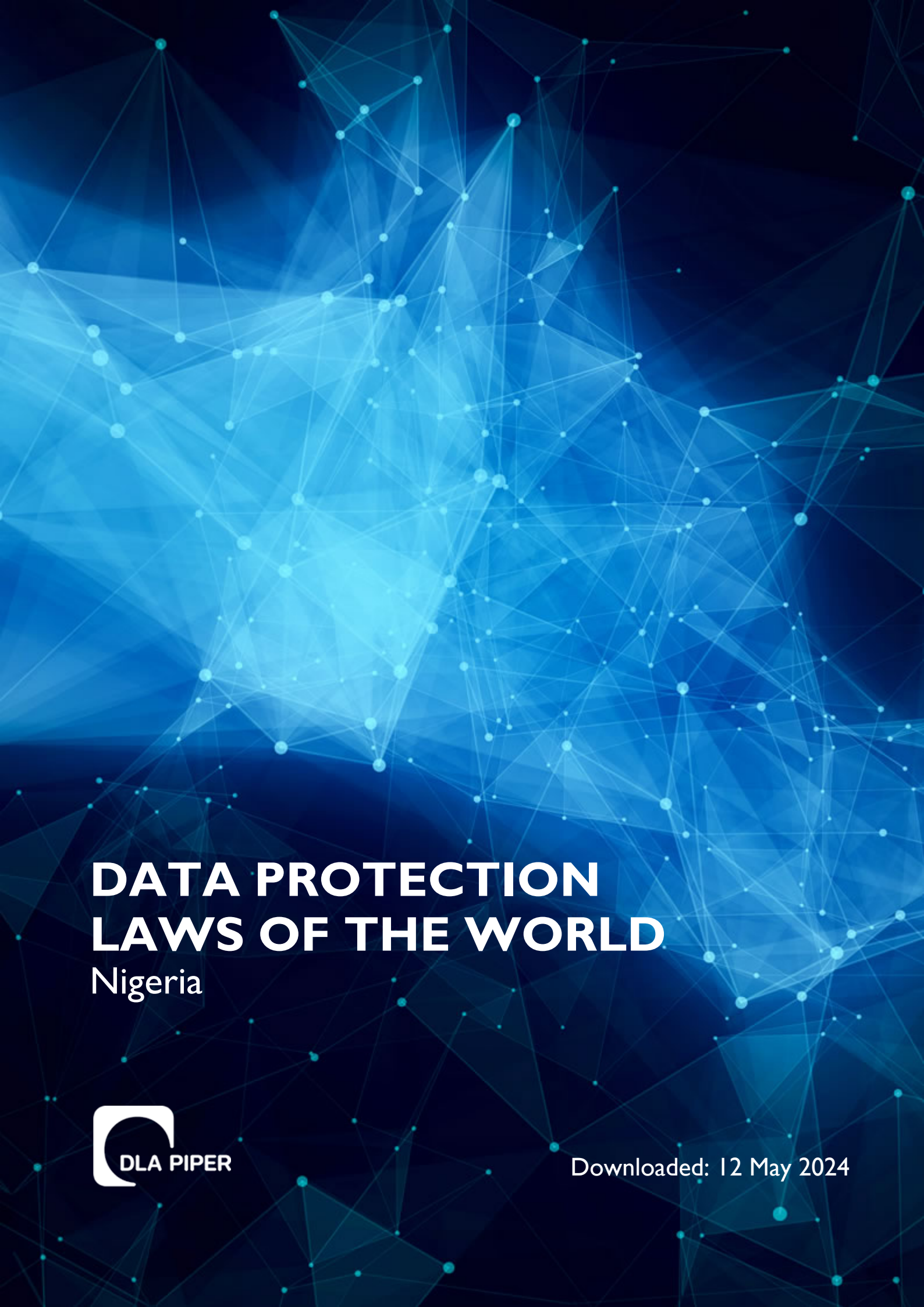
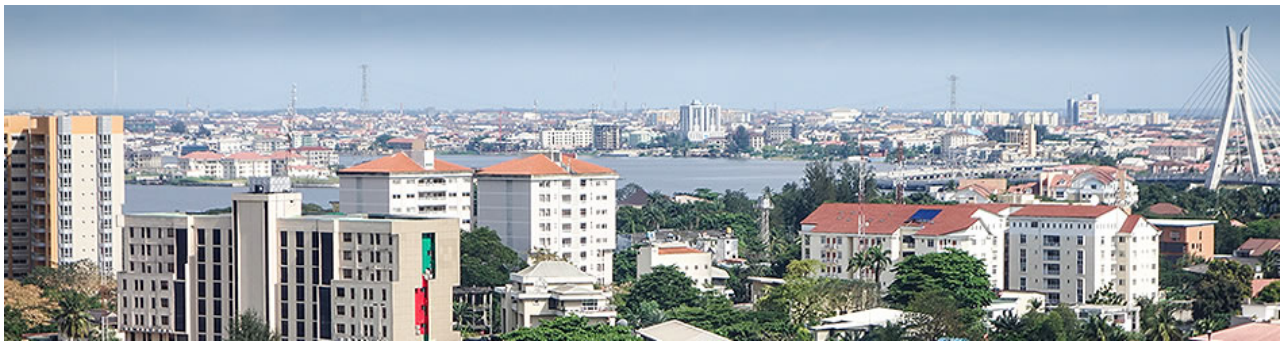


DATA PROTECTION LAWS OF THE WORLD

Nigeria

DLA PIPER

NIGERIA



Last modified 18 January 2024

LAW

Principal regulation

Data Protection Act

The Act has been enacted to safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria. Among other things, the objective of the Act include: the protection of personal information; establishing the Nigeria Data Protection commission for the regulation of the processing of personal information; promoting data processing practices that safeguard the security of personal data and privacy of data subjects; protect data subjects’ rights, and provide means of recourse and remedies, in the event of the breach of the data subject’s rights; and strengthening the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data etc. The Data Protection Act received Presidential assent on 13 June 2023.

Subsidiary legislation

Nigeria Data Protection Regulation

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

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 such PIs have access to the personal data 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. Key provisions in the mentioned laws are outlined hereunder:

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. Under the Act / Laws, age of a child is any person under the age of 18.

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 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 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 (NH) Act 2014

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 subscribers

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.

DEFINITIONS

Definition of personal data

Personal Data is defined as any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual. 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 personal data breach

Personal Data Breach is defined as a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Definition of data subject

Data Subject means a person to whom personal data relates.

Definition of data controller

Data Controller means a person, private entity, public commission, agency or any other body 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.

Definition of Sensitive Personal Data

Sensitive Personal Data means personal data relating to any of the following:

- genetic and biometric data, for the purpose of uniquely identifying a natural person;
- race or ethnic origin;
- religious or similar beliefs, such as those reflecting conscience or philosophy;
- health status;
- sex life;
- political opinions or affiliations; and
- trade union memberships.

NATIONAL DATA PROTECTION AUTHORITY

Nigeria Data Protection Commission

The Nigeria Data Protection Commission (the Commission) was established under the Nigeria Data Protection Act 2023 (the Act) as the supervisory and regulatory authority for data protection in Nigeria, a function previously undertaken by the Nigeria Data Protection Bureau (NDPB). Essentially, the Commission is the successor-in-title to the duties, power and functions of the NDPB.

REGISTRATION

Data controllers and data processors of major importance must register with the Commission within six months after the commencement of the Act or of becoming a data controller or data processor of major importance. Data controller or data processor of major importance is defined under the Act to mean a data controller or data processor that is resident or operating in Nigeria and processes the personal data of more than such number of data subjects who are within Nigeria as the Commission may prescribe, or such other class of data controller or data processor processing personal data of particular value or significance to the economy, society or security of Nigeria, as the Commission may designate. The Act even though it defines data controllers and data processors of major importance it does not define the measure of processing that would classify a controller or processor as being of major importance. It is likely that regulations issued by the Commission in the future will address this.

DATA PROTECTION OFFICERS

The Nigerian Data Protection Act 2023 requires Data Controllers to designate a Data Protection Officer (**DPO**) who will be responsible for ensuring internal compliance with the Act, other applicable data protection directives, and serving as a point of contact between the Data Controller and the regulatory body (Nigeria Data Protection Commission). The Data Protection Officer may be an employee of a Data Controller or engaged by a service contract.

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; and
- 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 and the data is processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach;
- Processing is necessary for compliance with a legal obligation to which the Controller is subject under;
- 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 contract to which the Data Subject is party to or in order to take steps at the request of the Data Subject prior to entering into a contract; and / or
- Data processing by a third party is governed by a written contract between the third party and the authorised Data Controller. Accordingly, any person engaging a third party to process the data obtained from Data Subjects shall ensure compliance with the Nigerian Data Protection Act 2023.

TRANSFER

The Data Protection Act on transfer of personal data has provided that such transfer is permissible if the recipient of the data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data.

To ensure the level of adequacy required by the recipient country of personal data, the following will occur:

- a data controller or processor shall record the basis for transfer and adequacy of protection in that country;

- the Commission may make regulations requiring data controllers and processors to notify it of the measures in place to explain their adequacy in accordance with the Act;
- the Commission may by regulation designate categories of personal data that are subject to additional specified restrictions on transfer to another country based on the nature of such personal data and risks to data subjects.

Other forms of assessment to be taken into account to ensure adequacy of protection include:

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

The Commission shall issue guidelines for these assessments in line with the factors that have been outlined above. The Commission may determine if a country, region or specified sector within a country has the adequate level of protection. The Commission may approve binding corporate rules, codes of conduct, certification mechanisms or similar instruments for data transfer proposed to it if it meets the standards specified in this Act.

In the absence of adequacy of protection as specified by the Act, transfer of personal data from Nigeria to another country is possible if at least one of the following conditions are met:

- The data subject has provided and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections;
- transfer is necessary for the performance of a contract to which a data subject is a party or in order to take steps at the request of a data subject, prior to entering into a contract;
- transfer is for the sole benefit of a data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer or if it were reasonably practicable to obtain such consent, the data subject would likely give it;
- transfer is necessary for important reasons of public interest;
- transfer is necessary for the establishment, exercise, or defense of legal claims; or
- transfer is necessary to protect the vital interests of a data subject or of other persons, where a data subject is physically or legally incapable of giving consent.

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 an obligation on a data processor, on becoming aware of a breach to do the following:

- notify the data controller or processor that engaged it, describing the nature of the personal data breach including where possible, the categories and approximate number of data subject and records concerned;
- respond to all information requests from the data controller or processor that engaged it;
- within 72 (seventy two) hours of becoming aware of a breach, if the breach is likely to result in a risk to the rights and freedoms of individuals, the data controller is obligated to notify the Commission. The data controller will immediately

communicate the breach in plain and clear language including advice about measures the data subject could take to mitigate the effect of the breach. In the event that it is not feasible, a public communication in one or more widely used media sources in which the data subject will likely be informed, can be used.

ENFORCEMENT

The Commission is saddled with supervisory and enforcement responsibilities in respect of data protection matters in Nigeria. It collaborates with security agencies like the office of the Inspector General of Police to ensure full compliance and enforcement. Where the Commission is satisfied that a data controller or data processor has violated or is likely to violate any requirement under the Act or any subsidiary legislation, the Commission may make an appropriate compliance order against that data controller or data processor. The order made by the Commission may include:

- warning that certain act or omission is likely to be a violation of one or more provisions under the Act or any subsidiary legislation or orders issued under it;
- requirement that the data controller or data processor complies with such provisions, including complying with the requests of a data subject to exercise one or more rights under the Act; or
- cease and desist order requiring the data controller or data processor to stop or refrain from doing an act, which is in violation of the Act, including stopping or refraining from processing personal data that is the subject of the order.

If the Commission, after completing an investigation, is satisfied that a data controller or data processor has violated any provision of the Act it:

- may make any appropriate enforcement order or impose a sanction on the data controller or data processor; and
- shall inform the data controller or data processor, and if applicable, any data subject who lodged a complaint leading to the investigation, in writing of its decision.

An enforcement order made or sanction imposed shall include:

- requiring the data controller or data processor to remedy the violation;
- ordering the data controller or data processor to pay compensation to a data subject, who has suffered injury, loss, or harm as a result of a violation;
- ordering the data controller or data processor to account for the profits realised from the violation; or
- ordering the data controller or data processor to pay a penalty or remedial fee.

Applicable remedial fees are as follows:

- For data controllers / processors of major importance, the organization can be fined up to 2% of its annual revenue or 10 million Naira, whichever is greater;
- In case of a data controller / processors not of major importance, the organization can be fined up to 1% of its annual revenue or 2 million Naira, whichever is greater.

Also, a data controller or data processor, who fails to comply with orders made by the Commission commits an offence and is liable on conviction to — (a) a fine of up to the — (i) higher maximum amount, in the case of a data controller or data processor of major importance, or (ii) standard maximum amount, in the case of a data controller or data processor not of major importance; or (b) imprisonment for a term not more than one year or both.

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 must be specified.
- 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 Advertising Regulatory Council of Nigeria Act 2022 (ARCON Act) is the apex law regarding advertising and marketing communications in Nigeria; its scope covers both terrestrial and online advertisements. The Nigerian Code of Advertising Practice Sales Promotion and Other Rights / Restrictions on Practice (5th Edition) which continues in force under the ARCON Act, provides 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 as safeguarded by the constitution may be subject to civil enforcement under the Fundamental Rights Enforcement Procedure Rules, 2009.

According to the Nigeria Data Protection Act, data controllers are obligated to perform a data privacy impact assessment where processing personal data could potentially pose a substantial risk to the rights and freedoms of a data subject, taking into

consideration the nature, scope, context and purposes of such processing. Where the probability of high risks is established by the impact assessment, the controller is obligated to consult the Commission before processing.

The Nigeria Data Protection Regulations 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 violation;
- Timeframes associated with available remedies; and
- 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.