FACTSHEET: NIGERIA

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 204,537,814
Capital: Abuja
President: Muhammadu Buhari
2020 Freedom House Score: 47/100
Data protection law? Enforced

LAW

Section 37 of the 1999 Constitution of the Federal Republic of Nigeria, provides for the right to privacy. Twenty years later, in 2019, the National Information Technology Development Agency (NITDA) released the Nigeria Data Protection Regulation (NDPR), both to safeguard the rights of Nigerian citizens and to keep Nigerian businesses competitive globally. As of April 25, 2019, all public and private organisations that process personal data must publicise their NDPR compliant data protection policies. As of July 25, 2019, organisations must conduct an initial audit or their privacy and data protection practices.

In terms of the NDPR, data subjects have the right to:

- object to the processing of their personal data for marketing purposes;
- access their personal data (and have personal data transferred to another data controller);
- obtain information about the processing of their personal data;
- have their personal data deleted (where certain criteria are met);
- have their personal data corrected;
- restrict the processing of their personal data (where certain criteria are met);
- withdraw consent to the processing of their personal data; and
- lodge a complaint with the NITDA or another relevant regulator.

While the principles in the NDPR appear to be well-considered, most countries that enact comprehensive data protection legislation simultaneously create an independent regulatory body to enforce and oversee the regulation. Nigeria has not done so, instead tasking NITDA with the enforcement of the NDPR. It remains to be seen whether there is enough bandwidth within NITDA to handle NDPR enforcement and perform all of its pre-existing duties, but regardless, the statutorily-mandated scope of NITDA's authority (to, "develop Regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour and other fields, where the use of electronic communication may improve the exchange of data and information") may not be broad enough to allow the agency to perform responsibilities such as charging fines to entities that violate the NDPR. Furthermore, because NITDA is an executive agency, NDPR provisions can be superseded by any act of Parliament.

PERSONAL DATA

Personal data means any information relating to a data subject. It could be a name, address, photo, email address, bank details, posts on social networking websites, medical information, or unique identifier such as a MAC address, IP address, IMEI number, IMSI number, SIM, etc.

Sensitive personal data means data relating to:

- religious or other beliefs;
- health or sexual tendencies;
- race or ethnicity;
- political views or trades union membership;
- criminal records; or
- any other sensitive personal information.

COLLECTION AND PROCESSING

Personal data must be collected and processed for a specific, legitimate and lawful purpose consented to by the data subject:

- Before personal data is collected, 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 processing.
- The legitimate interests of the controller or third party must be stated, along with the recipients of the personal data, if any.
- If personal data is being transferred to another country or international organisation, the data subject should know of the existence or absence of an adequacy decision by NITDA, and the period for which personal data will be stored.
- Data subjects must be informed of their rights to access and rectify personal data, withdraw consent for further processing at any time, and file a complaint with the relevant authority.
- The data controller must provide data subjects with any relevant information on any different additional purpose prior to further processing

For personal data processing to be lawful, at least one of the following must apply:

- The data subject has consented to the processing of personal data for one or more specific purposes.
- Processing is necessary to perform or enter a contract to which the data subject is party.
- Processing is necessary for the controller to comply with a legal obligation.
- Processing is necessary to protect the vital interests of the data subject or another natural person.
- Processing is necessary to perform a task crucial to the public interest or to exercise an official public mandate vested in the controller.
- If a third party is processing the data, a written contract between the third party and the data controller, and the third party is compliant with the Regulation

REGISTRATION AND ENFORCEMENT

Data controllers must appoint a data protection officer (DPO) to facilitate compliance with the NDPR and implement relevant data privacy instruments and data protection directives for the data controller.

NITDA is responsible for registering and licensing Data Protection Compliance Organisations (DPCOs) to monitor, audit, conduct training and data protection compliance consulting to all data controllers on behalf of the Agency.

Audits are required to be submitted to NITDA:

- when a data controller processes personal data of more than 1000 people in 6 months; or
- annually, by March 15, when a data controller processes personal data of more than 2000 people in a year.

The NDPR states that any entity found to be in breach of the privacy rights of any data subject will be liable, in addition to any other criminal liability, for the following:

- for data controllers "dealing with more than 10,000 data subjects," a fine of 2% of annual gross revenue of the preceding year or 10 million Naira, whichever is greater; or
- for data controllers "dealing with less than 10,000 data subjects," a fine of 1% or 2 million Naira, whichever is greater.

In terms of the NDPR, NITDA and relevant authorities will also develop international cooperation mechanisms to facilitate the effective enforcement of the legislation outside of Nigerian borders.

CROSS-BORDER TRANSFER

For an extra-territorial transfer of personal data to occur, NITDA must decide that the jurisdiction, sector, or the organisation in question grants an adequate level of protection, and the Attorney-General must also perform an analysis of the legal system of the jurisdiction taking numerous considerations into account. Absent a decision by either NITDA or the Attorney-General, such a transfer shall take place only if:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks;
- the transfer is necessary for the performance of a contract to which the data subject is a party; or
- the transfer is necessary for the public interest, legal claims, or to protect the vital interests of the data subject or of other persons, where the data subject is incapable of giving consent

SECURITY AND BREACH PROTOCOL

Data processors and controllers are required to implement adequate technical and organizational security measures, such as:

- setting up firewalls;
- storing data securely with access to specific authorised individuals;
- employing data encryption technologies;
- developing organisational policies for handling personal data (and other sensitive or confidential data); and
- protecting emailing systems and continuously building capacity for staff.

Data must be protected from all foreseeable hazards and breaches such as theft, cyberattacks, viral attacks, dissemination, manipulations, as well as physical damage by rain, fire or exposure to other natural elements.

Read the legal notice and terms of use for this factsheet.