Demonstrating Compliance with the Nigerian Data Protection Regulation

The Nigerian Data Protection Regulation, 2019 ("NDPR") is the primary regulation on data privacy and data protection in Nigeria. It is complemented by the NDPR Implementation Framework (the "Framework") which is intended to clarify relevant provisions of the NDPR that need clarity. Importantly, the Framework does not supersede the NDPR. The NDPR provides for, among other things, the safeguard of the rights of natural persons to data privacy and fosters safe conduct for transactions involving the exchange of personal data.

The NDPR outlined various obligations which an organization must comply with as a way of demonstrating its compliance with the NDPR. These obligations, better described as the 'Accountability Obligations' are subsumed in Art. 2.1(3) of the NDPR which provides that "anyone who is entrusted with the personal data of a data subject or who is in possession of personal data of a data subject shall be accountable for his acts or omissions in respect of data processing, and in accordance with the principles contained in the NDPR". A data controller[1], therefore, has a unique task of ensuring that the handling or processing of personal data is in line the principles of processing personal data which are" Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality.

While the obligations of a data controller are embedded in the above principles, compliance by the data controller must be clearly demonstrated to ensure accountability. This can be expressed in the following ways:

a. Data Protection Policy and Privacy Notice

Art. 2.5 of the NDPR provides, among other things, that any medium through which personal data is being collected or processed shall display a simple and conspicuous privacy policy that the class of data subject being targeted can understand. This could be displayed in different forms on the organisation's website, conspicuous locations in the offices, etc.

Data Protection Policy differs from Privacy Notice in the sense that while the policy is an internal document that informs the organisation's employees how to protect the personal data of customers, the Privacy Notice is an external document that tells the organisation's visitors and customers how their data is collected, processed and their privacy rights. An organization should therefore have both an

[1] A Data Controller is 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.

internal privacy policy that will guide the internal operations of the organisation, and a privacy notice that will guide its relationship with customers and visitors.

b. Designation of a Data Protection Officer

A Data Protection Officer ("DPO") is a person or agency within or outside an organization whose responsibility is to ensure that the organization is correctly protecting individuals' personal data in accordance with existing legislation. Art. 4.1(2) of the NDPR provides that every Data Controller shall designate a DPO for the purpose of ensuring adherence to the NDPR, relevant data privacy instruments and data protection directives of the Data Controller.

Similarly, Art. 3.4.1 of the Framework mandates every data controller to appoint a dedicated DPO within 6 months of commencing business or within 6 months of the issuance of the Framework, where one or more of the following is present:

a. The entity is a government organ, ministry, department, institution or agency;
b. The core activities of the organization involve the processing of the personal data of over 10,000 subjects per annum;
c. The organization processes sensitive personal data in the regular course of its business; or
d. The organization possesses critical national information infrastructure (as defined under the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 or any amendment thereto) consisting of personal data.

Also, a Nigerian subsidiary of a multinational company to which the requirements stated above apply, is obligated to appoint a DPO who shall be based in Nigeria and shall be given full access to the management in Nigeria. The DPO of the Nigerian subsidiary may report to a global DPO where such exists.

The roles of a DPO cannot be overemphasized. A DPO is expected to ensure, in an independent manner, that an organization applies the laws protecting individual personal data. The DPO's position within an organization is imperative that it may be outsourced to a competent firm or person to handle.

The roles of a DPO are specifically provided for under Art. 3.7 (c) of the Framework as follows:

i. To inform and advise the organization, Management, employees and third party processors of their obligations under the NDPR;

ii. To monitor compliance with the NDPR and with the organization's own data protection objectives;

iii. To assign responsibilities, raise awareness and train members of staff involved in processing operations;

iv. Advice on data protection impact assessment and monitor its performance; and

v. Liaise with NITDA (NDPB) and/or DPCO on data protection matters.

A DPO must possess the requisite experience and specialization, with due regard to the nature of the organization processing activities and data protection issues that arise within the organization.

c. Trainings

An organization is obligated to provide periodic trainings to its personnel on its legal data protection obligations and policy requirements. Advisedly, the trainings should be designed to align with the business operations of the organisaiton and the individual roles of different employees. Art. 4.1(3) of the NDPR provides that a Data Controller or Processor shall ensure continuous capacity building for DPOs and the generality of her personnel involved in any form of data processing. Best practice is for the training content to cover the key areas of data protection mechanisms including data retention, incident detection and response, information security, etc.

d. Data Protection Audit

The true essence of the NDPR and most importantly, the accountability obligation of the organization will not be achieved if there is no practicable way of measuring or assessing compliance. Therefore, a data protection audit is necessary for assessing whether an organization is complying with its obligations. It also serves as a means for identifying data protection risks and prescribing recommendations for best practice. A Data Controller who processes the personal data of more than 2,000 data subjects in a period of 12 months is obligated to submit on an annual basis, summary of its data protection audit to the Nigerian Data Protection Bureau (NDPB), not later than the 15th of March of the following year[2].

[2] The NDPB extended the deadline for the year 2023 filing to June 30th, 2023.

The Role of the DPCO in Demonstrating Compliance with the NDPR

A DPCO is an entity duly licensed by the NDPB for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with the NDPR or any foreign Data Protection Law or Regulation having effect in Nigeria. A DPCO is, therefore, saddled with the responsibilities of:

a. monitoring organisation's compliance with extant laws and regulations on data protection;
b. conducting data protection audit;
c. drafting and review of data protection policies;
d. conducting training programs for DPOs and Data Controllers on data protection and privacy practices; and
e. data protection compliance consulting to Data Controllers under the NDPR or any foreign Data Protection Law or Regulation (such as the General Data Protection Regulation – GDPR) having effect in Nigeria.

Lexsetters is a licensed DPCO and can assist an organisation with the above listed matters.

Penalty for Default

Art. 2.10 of the NDPR provides for the fines that may be imposed on an organisation in respect of breach of the NDPR. It states that any person subject to the NDPR who is found to be in breach of the data privacy rights of any Data Subject shall be liable, in addition to any other criminal liability, to the following:

a. In a case of Data Controller dealing with more than 10,000 data subjects, the payment of a fine of 2% of the organization's annual gross revenue of the preceding year or the payment of the sum of N10,000,000.00 (Ten Million Naira) whichever is greater, and

b. In the case of a Data Controller dealing with less than 10,000 Data subjects, the payment of a fine representing 1% of the organization's annual gross revenue of the preceding year or payment of the sum of N2,000,000.00 (Two Million Naira), whichever is greater.

No part of this article should be relied upon as legal advice. It is only intended as a general guide on the subject and as such, we advise that you consult a lawyer where legal advice is desired.

Key Contacts

Ogobuike Emmanuel Umoke
Associate
oumoke@lexsetters.com

Kelechi Attamah
Partner
kelechi@lexsetters.com