

NEWSLETTER



The 2019 Nigerian Data Protection Regulation: A Protectionist Initiative from the NIDTA

The NIDTA Data Protection Regulation

There have been several advances in business technology in the past decades, most of which have been validated by far reaching internet access, improved software development tools and the reliability of data centers. Many countries have enacted laws to keep up with the trends of technology in business and its implications. The General Data Protection Regulation 2018 (GDPR), applicable to all European Union (EU) members easily comes to mind as the benchmark enactment for the protection of personal data.

In line with current realities and global standards, Nigeria has joined the league of countries adopting stricter legislation on data protection with the enactment of the Nigerian Data Protection Regulation 2019 (the Regulation/NDPR), the latest initiative conceived by the National Information Technology Development Agency (NITDA).

Although there are existing laws on data privacy, the Regulation specifically prescribes the minimum data protection requirement for the collection, storage, processing, management, operation and technical control of personal data in Nigeria. It may also be the strictest and most far reaching data law passed in Nigeria, imposing stringent conditions on companies and stiff penalties on defaulters.

What and Who does the Regulation Apply to?

All transactions in which the personal data of natural persons resident in Nigeria, or natural persons outside Nigeria of Nigerian descent, is being processed come under the purview of the Regulation. It equally applies to government agencies and institutions, and private sector organisations that own, use or deploy information systems as well as organizations based outside Nigeria if such organisations process personal data of Nigerian residents.

The Regulation provides for two different types of data-handlers: 'data administrators' and 'data controllers'. A data controller is defined as 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 while data administrators are persons or organizations who process data.

Key obligations of the Regulation

a. Consent Obligation

Under the terms of the Regulation, a double obligation of disclosure and consent is imposed on the Data Controller providing that no data shall be obtained or processed except the specific purpose of collection is made known to the Data Subject (anyone whose personal data is being collected, held or processed). The Data Subject's consent must have been obtained prior to collections and such consent secured without fraud, coercion or undue influence.

The subject of consent is a sensitive one as the Regulation envisages that the Data Subject has made a deliberate choice to share his personal information for processing. In the event that such consent was obtained under irregular circumstances, same would be null and void. It is important to note that the Data Subject has a right to withdraw his/her consent at any time, and must be informed of this right and the method to withdraw any prior given consent with ease.

According to the NDPR, consent could be obtained through a statement or a clear affirmative action. A typical example of this is when a user on a website platform clicks "I understand and I accept" after reading (or least after being shown) a privacy statement or cookie consent.

b. Right to be Forgotten

The right to be forgotten or the right to erasure appears in Articles 3.9 and 3.10 of the NDPR. It grants the Data Subject the right to request the

Contact Us:

Abuja Office

Afri-Investment House
Plot 2669 Aguiyi Ironsi Street,

Cadastral Zone 06,

Maitama Abuja

+234 09 291-7347

Lagos Office

1B Utomi Airie Avenue,

Off Admiralty Way,

Lekki 1, Lagos.

+234(0) 9059 7777 34

+234(0) 9059 7777 35



Author:

Uche Odigili

(Associate at Primera Africa Legal)

Controller to delete Personal Data without delay, and the Controller is bound to delete such Personal Data where one of the stated grounds applies. Where the Controller has made the Personal Data public and is obliged to delete the Personal Data, he must take all reasonable steps, to inform Controllers processing the Personal Data of the Data Subject's request.

Whereas the GDPR cites specific reasons which trump the right to erasure, the NDPR simply takes the ambiguous route by stating that *"The exercise of the foregoing rights shall be in conformity with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights"*

c. Publicity and Clarity of Privacy Policy

A privacy policy is mandatory under the NDPR and the requirements and content of such policy explicitly stated. The policy must be simple and easy to understand, and visible to anyone whose data is targeted. A good example of such clearly written privacy policy is Google's which utilizes concise lists, visuals and short sentences that easily complies with its corresponding privacy policy requirement.

A privacy policy that is compliant with the NDPR should include the nature of the Data Subject's consent, description of collectable personal information, purpose of collection of Personal Data, technical methods used to collect and store personal information, cookies, JWT, web tokens etc. Although not stated in the NDPR, it is usually advised that privacy policies should avoid using qualifiers such as "may", "might", "some", "often" as they are purposely vague.

It is important to disclose that the NDPR demands that every Data Controller should as at 25 April 2019 (three months after the Regulation was issued) publish its data protection policy.

d. Privacy and Data Protection Audit

Another time-based requirement from the Regulation is the obligation of each organization to conduct a detailed audit of its privacy and data protection practices. Such audit must be conducted within 6 months of the issuance of the Regulation (which means the first of such audit should have been conducted on or before July 25, 2019). Article 4.5 (a-i) contains the least content expected of these audits.

Where a Data Controller processes the Personal Data of more than 1000 persons within a period of six months, that Data Controller is expected to forward a soft copy of the summary of the audit to the Agency (NITDA). Also, a Data Controller who processed the Personal Data of more than 2000 Data Subjects in a period of 12 months shall, not later than the 15th of March of the following year, submit a summary of its data protection audit to the Agency. This is to be done on a yearly basis.

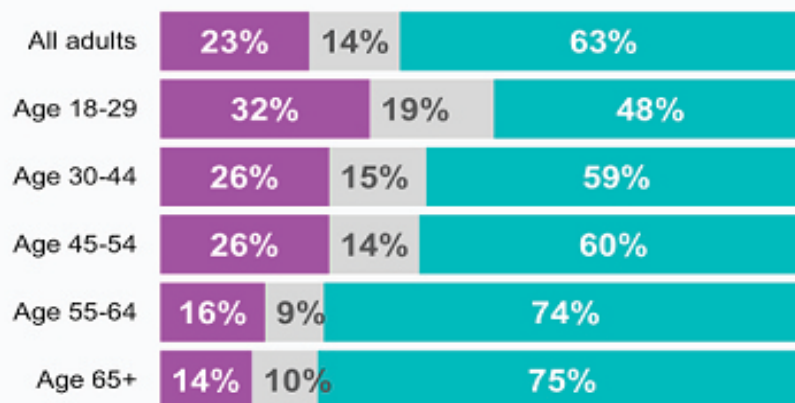
e. Appointment of a Data Protection Officer

One of the important provisions of the NDPR is the obligation of Data Controllers to appoint a Data Protection Officer. This individual is responsible for supervising the strategy behind data protection and ensuring a company is compliant with the Regulation. He/she is also in charge of instructing and training the company's

How Adults of Different Ages Feel About Data Privacy

How willing would you be to give a company access to your personal data for targeted advertising if it meant you could use their service for free?

■ Willing ■ Don't Know / No Opinion ■ Not Willing



"If you're not paying, you are the product"

employees on what's required of them and their organization, and acts as the contact between the organization and the regulatory authorities. On the other hand, NITDA has been empowered to appoint, register, and license Data Protection Compliance Organisations (DPCOs) who shall on behalf of the Agency monitor, audit, conduct training and data protection compliance consulting to all Data Controllers.

Interestingly, the Regulation empowers the mass media and the civil society with the right to uphold accountability and foster the objectives of this Regulation. It remains to be seen how this will pan out.

f. Transfer of Data to Third Party Countries

The Regulation envisages cases where data may have to be transferred to third party countries or international organisations. Any transfer of Personal Data in this regard is subject to the supervision of the Honourable Attorney General of the Federation (HAGF) who would typically consider the reflection of Nigerian laws and approach to data protection in these foreign territories. A transfer may also be approved if NITDA concludes that the third-party destination of the data ensures adequate protection. In the event that neither NITDA nor the HAGF are certain as to the adequacy of safeguards for data processing in a foreign country or an international organisation, the data controllers may still be able to process and transfer data provided any one of the set conditions are met.

Penalties

Unlike the GDPR where fines depend on the severity of the breach, the Regulation

focuses on the number of data subject affected.

In the case of a Data Controller dealing with more than 10,000 Data Subjects, defaulters are liable to payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater. Where the Data Controller is dealing with less than 10,000 Data Subjects, such data controller shall be liable to a payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater. It is instructive to note that the payment of these fines does not absolve the defaulters of any criminal liabilities.

CONCLUSION

Increased commercial activities along digital platforms have led to a greater risk of data mismanagement and exposure of customers and clients. The NITDA therefore deserves some accolades for issuing an updated legal framework to secure personal data protection in Nigeria. Though the NDPR still has some gaps when compared with what obtains in other jurisdiction (the GDPR, for instance), it is a welcome development, especially in the light of recent scandals that have weakened people's trust in how organisations process personal data.

It is important for companies that collect and process data to be familiar with the terms of the NDPR as the consequences for non-compliance could be dire.

Operators protest against tax on GSM, cable TV subscription

Telecommunications operators have kicked against plans by the National Assembly to impose taxes on global system for mobile (GSM) and cable television subscriptions and services in the country. Under the aegis of the Association of Telecommunications Companies of Nigeria (ATCON), the body said imposing such tax now would amount to double taxation, and subsequently impact the economy negatively.

Aramco, ADNOC mull investments in Nigeria's energy sector

State-owned energy firms Saudi Aramco, and Abu Dhabi National Oil Co. are mulling investing in Nigeria's energy sector, including potential supply of gasoline to West Africa through Nigeria, the Group Managing Director, Nigerian National Petroleum Corporation (NNPC), Mele Kyari, said on Tuesday. Teams from ADNOC and NNPC met in Abu Dhabi this week, to discuss investment opportunities that could range from upstream to midstream to downstream, Kyari told reporters at an industry event in Fujairah in the United Arab Emirates (UAE).

FG mulls return of toll gates to drive infrastructure development

Fifteen years after 31 toll plazas constructed at an average cost of N1 million each were demolished on the orders of the Federal Government, the government says plans are on to return the tollgates in order to encourage private sector participation in the development of basic infrastructure in the country.

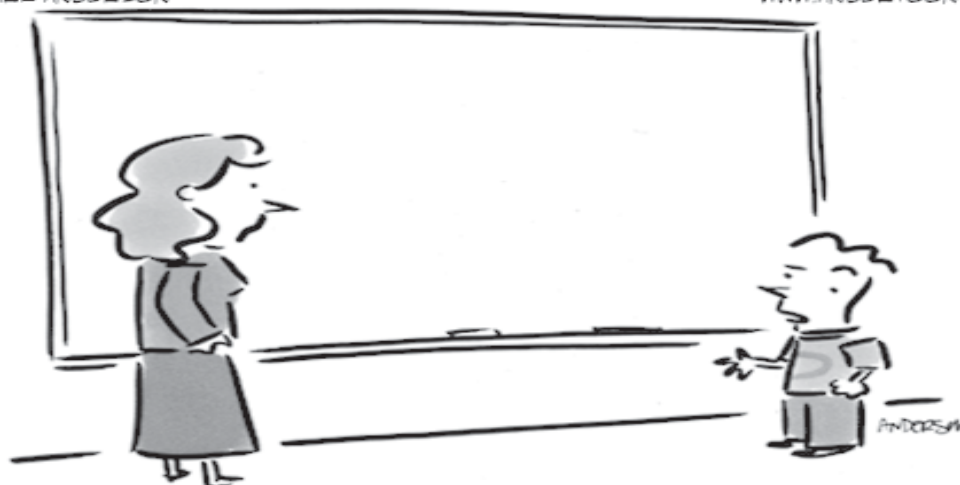
On A Lighter Note

THE INCHOOERS



© MARK ANDERSON

WWW.ANDERTOONS.COM



"Before I write my name on the board, I'll need to know how you're planning to use that data."

Senate moves to amend PSC Act, probe N7 trn FG's oil revenue loss 20 years after.

The Senate on Wednesday resolved to quickly amend the Production Sharing Contract (PSC) Act in order to end the years of oil revenue loss to the Federal Government. The resolution follows several failed efforts by the 8th Senate to review the Act through private members and government-sponsored bills.

US Justice Department closes investigations on Eni's Nigerian, Algerian cases

The United States Department of Justice (DOJ) would be taking no action against Eni as it shelved investigations into corruption allegations against the Italian oil major in the purchase of a Nigerian oil field in 2011, the company said. The DOJ also closed a graft case in Algeria against the oil company in a similar fashion.

Editor-in-Chief:

Fatima Aigbomian

Editorial Board :

Nonso Nkamuke

Hannatu Babatunde

Kiadum Nwakoh

Associate Editors:

Tosin Amusan

Priscilla Babudoh

Disclaimer: The content of this Newsletter does not constitute legal advice. Should you have any questions regarding the issues discussed, please send an email to iaye@primeraal.com or to your contact at Primera Africa Legal