FREQUENTLY ASKED QUESTIONS (FAQs) ON THE NIGERIA DATA PROTECTION REGULATION 2019

*1. **What specific objectives is the Regulation meant to achieve?***

Aside from the expressed objectives in Article 1 of the Regulation, the Regulation hopes to stimulate a Data Protection Service sector. The Regulation adopts an indirect oversight approach. This would provide opportunities for qualified persons to engage in requisite services for Data Controllers at a cost. NITDA believes that by unlocking this sector, thousands of jobs would be created.

Another major objective is to reduce the barriers of Nigerian businesses to global opportunities. The Nigeria Data Protection Regulation (NDPR) has adequately dealt with the cardinal issues of consent of Data Subject; lawful processing; prohibition of atrocious motives; clarity of privacy policy; third party data processing; penalty for default; definition of Personally Identifiable Data and Data Privacy Breach remediation mechanism among many others. The Regulation in effect meets the minimum standards required for transborder data processing. This Regulation would help Nigerians to engage freely with other foreign businesses upon compliance with a home-grown data regulatory regime.

*2. **The NDPR covers transactions intended for the processing of personal data and to actual processing of personal data and person(s) residing in Nigeria or residing outside Nigeria but of Nigerian descent. But unlike the EU's General Data Protection Regulation (the "GDPR"), it appears that the NDPR does not apply to persons and entities outside Nigeria that collect, store, or process data of persons in Nigeria.***

The NDPR is crafted to be pragmatic in expectation and enforcement. While the incidence of foreign data breach is not in doubt, the NDPR seeks to grow its regulations and enforcement organically. Most of the major data processors such as Google, Facebook, WhatsApp etc. all have a Nigerian office, in that regard, the enforcement would apply to them when in breach even outside Nigeria. Furthermore, aside from this Regulation, Nigeria has Mutual Legal Assistance Agreements with

most countries, which would make it possible to still go after foreign data breaches if the country feels the need to do so.

3. Has the Regulation come into effect and when does the 6-months grace period expire?

The Regulation has come into effect since 25th January, 2019. A major advertorial was carried in four major national dailies between 14th and 15th of February, 2019 to sensitize people on this. The grace period would elapse by 25th of July, 2019.

4. The Regulation places too much emphasis on data collection and processing but does not adequately address the issue of data retention, why is this so?

Processing was defined in Article 1.3(r) as follows:

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; …

Any reference to processing in the Regulation applies to data storage or retention. Modern legal drafting styles detest prolixity and verbosity. Since *processing* has been defined, any reading of it in the Regulation must refer to its definition except expressly stated otherwise.

5. What is the legislative competence of NITDA to issue data regulation? Will a regulation issued by NITDA stand in court?

NITDA is empowered to regulate electronic data use in Nigeria. Section 6(a and c) of the NITDA Act 2007 makes this clear.

The Agency Shall-

(a) Create a frame work for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto

(c) Develop guidelines 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.
This provision makes it clear that NITDA has the authority to regulate data from any electronic or digital platform.

A breach of NITDA regulation is a breach of the NITDA Act as provided by Section 17 and 18 of the Act. Therefore, a breach of this Regulation is enforceable in the Nigerian court.

6. Our business operates an international model, wherein customer's data are transferred across borders often, how does the NDPR impact on this model?

The NDPR recognizes the need for cross-border transfer of data in an era of globalized and high-speed business transactions. Article 2.11 of the Regulation, which relates to Transfer to a Foreign Country, addresses this concern. To comply with the provision and other aspects of the Regulation, the Data Controller would provide the following:

i. The List of Countries where personally identifiable information of Nigerian citizens are transferred in the regular course of business.

ii. The Data Protection laws and contact of National Data Protection Office/Administration of such countries listed in i) above.

iii. The privacy policy of the Data Controller, compliant with the provisions of the NDPR.

iv. Overview of encryption method and data security standard

v. Any other detail that assures the privacy of personal data is adequately protected in the target country.

7. Does the NDPR mandate businesses to host data only on local servers?

The NDPR does not mandate private businesses to host data only on local servers, although this is highly encouraged. Government data as well as critical national data in the custody of private organisations must however be hosted in-country. Where hosted abroad, the Data Controller, should however, provide NITDA with the countries where such servers are located and their data protection policies.

8. Would data privacy audits conducted by private auditors be compliant to the NDPR?

NITDA does not accept audit report by non-licensed third-party auditors. The Data Controller may encourage its auditors to obtain the Data Protection Compliance Organisation (DPCO) license or alternatively deal with NITDA licensed DPCOs. Every audit report required under the Regulation must be accompanied by a Verification Statement by a licensed DPCO.

9. When are Data Controllers expected to file data protection audit report?

Except for other specified purposes or request by NITDA, Data Controllers are expected to file their data audit report annually before the 15th of March of the following year.

10. What is the role of a Data Protection Compliance Organisation (DPCO)

A “Data Protection Compliance Organization (DPCO)” means any entity duly licensed by NITDA 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. In essence any organization that wishes to provide any form of data privacy protection service to Nigerian companies must acquire this license.

Submission of annual audit report by Data Controllers must be accompanied by a verification statement by a licensed DPCO.

11. Do Data Controllers wishing to transfer data abroad, obtain permission of the Attorney-General of the Federation before doing so?

Article 2.11 of the NDPR provides: *Any transfer of Personal Data which is undergoing processing or is intended for processing after transfer to a foreign country or to an international organisation shall take place subject to the other*

provisions of this Regulation and the supervision of the Honourable Attorney General of the Federation (HAGF).

Data Controllers do not require permission of the Attorney-General for every transfer of Data outside Nigeria. In transferring data abroad, Data Controllers shall provide the following information to NITDA through their annual audit report or where specifically requested by NITDA.

i. The List of Countries where Nigerian citizens personally identifiable information of Nigerian citizens are transferred in the regular course of business.

ii. The Data Protection laws and contact of National Data Protection Office/Administration of such countries listed in i) above.

iii. The privacy policy of the Data Controller, compliant with the provisions of the NDPR.

iv. General overview of the data protection mechanism to protect Nigerian citizens' data.

NITDA shall relate with the Office of the Attorney General of the Federation to seek guidance on Nigerian legal position on any aspect of the Regulation or where there is a breach of private data in a foreign jurisdiction.