Jul 2019

Nigeria: New regulation demonstrates a serious approach to data protection

On 25 January 2019, the National Information Technology Development Agency ('NITDA') issued the Nigeria Data Protection Regulation 2019 ('the Regulation'). Although it is a subsidiary legislation, the Regulation has the force of law, having been issued in accordance with the mandate of the National Information Technology Development Agency Act 2007 (the 'NITDA Act'). Senator Iyere Ihenyen, Lead Partner at Infusion Lawyers, provides insight into how the Regulation will work, and comments on the impact it will have on data protection within Nigeria.

phototechno/Essentials collection/istockphoto.com

In today's data-driven global economy, Nigeria clearly wants to safeguard the personal data of Nigerians wherever they are, regardless of the means of data processing, or the location of the data controller or processor.

Before the Regulation, Nigeria had the Guidelines on Data Protection 2013 ('NITDA Guidelines'). However, right from the inception of the NITDA Guidelines until the time they were repealed, there were doubts over their status, coupled with a lack of enforcement of them. The NITDA Guidelines were also not as comprehensive as the Regulation.

By having a stronger protective regime for data privacy, in tune with global best practices, Nigeria hopes to help boost international trade and commerce. At a time when transactions increasingly involve personal data processing, one of the objectives of the Regulation is to ensure that there are adequate safeguards in place. Also, the economic advantage to data protection is not lost on the makers of the Regulation. The scope of the Regulation and its penalties demonstrate this consciousness.

Scope of the Regulation

The Regulation brings all data processing transactions involving data subjects who are Nigerians, anywhere in the world, under the Regulation, regardless of where the data controller or processor is located. Considering the huge and ever-growing population of the Nigerian people, home and abroad, applying protection to the personal data of natural persons residing in Nigeria, and natural persons residing outside of Nigeria but who are of Nigerian descent, is a welcome development.

No data controller or data processor anywhere in the world should be under any mistaken impression that the Regulation does not apply to it. Similarly to how the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') deals with the personal data of EU citizens, the Regulation will also work to protect the personal data of Nigerians globally. Data controllers and data processors involved in any data breach affecting the personal data of Nigerians are liable to the penalties set out by the Regulation.

Of course, the universal scope of the Regulation will certainly be a tall enforcement hurdle for NITDA, and for the various relevant authorities in Nigeria whose responsibility it is to regulate personal data in various sectors. International cooperation must be vigorously pursued, otherwise the success of enforcement would be significantly affected.

Data protection authority in Nigeria

The Regulation does not recognise NITDA as the sole data protection authority ('DPA') in Nigeria, and rightly so. This is because apart from NITDA, there are other relevant authorities, or statutory bodies, mandated by law to deal with matters relating to personal data in Nigeria. Therefore, under every act, regulation, and guideline that relates to personal data protection, various Government agencies are typically designated as the DPA in their relevant sectors. For example, in Nigeria's financial services industry, where the Consumer Protection Framework 2016 and the Credit Reporting Act 2017 apply, the Central Bank of Nigeria is the DPA. Similarly, in the telecommunications industry, the Nigerian Communications Commission is the DPA.

There have been calls for the establishment of an overarching DPA in Nigeria, but there are administrative and political concerns. A Data Commission Bill was passed 16 May 2019 by the National Assembly, which was forwarded to the President for assent. If assented to by the President, the Data Commission Bill will establish Nigeria's Data Commission. The Data Commission will be responsible for protecting personal data and regulating the processing of personal data, and other related matters.

Procuring consent of a data subject

Considering the high rate at which data controllers process personal data without first obtaining the data subject's consent, it is good to see that processing personal data without the data subject's consent is prohibited. Subject to legitimate purposes, such as for the prevention of crime, to aid an investigation, or for a court order, the Regulation prohibits the processing of personal data without first obtaining the data subject's consent. Before transferring personal data to a third party for any reason, the data subject's consent must also be obtained. Also, seeking, giving, or accepting consent in order to directly or indirectly propagate anti-social conducts, atrocities, children's rights violations, criminal acts, and hate, is prohibited by the Regulation. This will impact mainly on Nigeria's telecommunications industry, where subscriber's personal data is often subject to daily abuse.

Due diligence by data controllers

It is good to note that data controllers and data processors are now liable for the actions or inactions of third parties who handle the personal data of data subjects protected under the Regulation. This will minimise negligence and recklessness on the part of a data controller and processor. As a party to a contract, a data controller or processor is required to take reasonable measures

to ensure that the other party does not violate the data processing principles under the Regulation. It must ensure that the other party is either accountable to NITDA or a DPA within or outside of Nigeria. As NITDA does not have power over data controllers and processors outside of Nigeria, under the Regulation, regulatory authorities who exercise control over data controllers and processors outside Nigeria will provide enforcement assistance to NITDA, or the relevant regulatory authority in Nigeria. Enforcing this will definitely be a major challenge for regulators.

If NITDA does succeed in developing international cooperation and mutual assistance towards effective enforcement of personal data protection legislation, the magnitude of this task would be minimised. The Regulation contemplates information exchange, complaint referral, and investigative assistance amongst DPAs across jurisdictions. Whether NITDA can pull this off is debatable. So far, we are not seeing those international co-operations happening. Even locally, we are yet to start witnessing enforcement.

Privacy policies and data security for protection of personal data

Data controllers are now mandated to have a privacy policy published on their website or any medium through which they collect or process personal data. This is good, but even better is the requirement that data controllers or processors must put data security measures in place to ensure data protection. Beyond policy statements, data controllers must put measures in place to protect the personal data they collect, process, store, or transfer. Though the Regulation does not stipulate penalties for failing to have these data security measures, should a data breach result from this failure, data controllers and processors will be liable to the same penalties stipulated for data breaches.

Rights of a data subject under the Regulation

The Regulation does a good job guaranteeing privacy rights, such as:

- right to access;
- right to object;
- right to withdraw consent;
- right to deletion or right to be forgotten; and
- right to data portability.

However, it does not adequately provide remedial procedures to data subjects. Merely listing these privacy rights without detailing the redress that must be made available by data controllers, to an aggrieved person for certain data breaches, creates uncertainty. This uncertainty may affect the extent to which data subjects are able to enforce their rights. Particularly in a jurisdiction where enforcing rights is a major challenge, ensuring easily accessible and free, or cheap, administrative enforcement mechanisms at the level of data controllers, and then at the level of relevant DPAs, should have been given better attention. For example, the Regulation gives data subjects the right to submit complaints to a DPA, but it is silent about applicable remedial procedures, administrative timelines, and specific remedies for redress. Establishment of the administrative redress panel ('the Panel') is a good idea, but this is a quasi-judicial process that typically applies after pursuing redress with data controllers has already failed.

Restrictions on and exceptions to international data transfer

While the administrative and supervisory roles given to NITDA and the Accountant General of the Federation ('the AGF') are understandable, given how sensitive international data transfer generally is, they are bound to create a serious bureaucracy inconsistent with global competitiveness. It is a relief therefore that the Regulation contains certain exceptions to NITDA's or the AGF's

supervision. By obtaining the data subject's consent by virtue of necessity, such as contract performance, implementation of pre-contractual measures, public interest, etc., data controllers effectively avoid the requirement of obtaining approval from NITDA and the AGF.

Penalty for data breach

Unlike the NITDA Guidelines, which did not contain any penalties apart from the general penalties stipulated under the NITDA Act, the penalties stipulated under the Regulation demonstrate that Nigeria is taking data protection more seriously. Under the Regulation, a data controller who deals with more than 10,000 data subjects shall be liable to pay a fine of 2% of its annual gross revenue ('AGR') of the preceding year, or pay NGN 10 million (approx. €25,000), whichever is greater. Similarly, for a data controller who deals with less than 10,000 data subjects, the data controller is liable to pay the fine of 1% of the AGR of the preceding year, or pay NGN 2 million (approx. €5000), whichever is greater.

Apart from the nationality issue, adopting a GDPR approach to both the scope and the penalties for data breaches is quite commendable, particularly when one considers Nigeria's huge and growing population, home and abroad. If efficiently and effectively enforced, this will certainly set Nigeria up as a leader within Africa in terms of data protection, but this won't be a walk in the park. NITDA must be prepared to effectively enforce penalties against data controllers and data processors who breach the privacy rights of data subjects under the Regulation. This is particularly so with organisations that process the personal data of Nigerians on global platforms. NITDA will definitely need international co-operation. The provisions of the Regulation are quite inadequate in this regard, as it expects NITDA to drive that process and put cross-border enforcement mechanisms in place.

Third-party violations and the data controller's liability to data subjects

By impinging liability on a data controller, the Regulation protects a data subject against third party violations. This will have a direct effect upon data controllers, as the excuse that the data subject's personal data is out of the data controller's control, will no longer be tenable. This is why the Regulation requires third party data processing contracts between data controllers and the partners they engage. Consequently, data controllers must now keep processors that they can trust as partners. By way of improvement, I think the Regulation should have listed certain exceptions in order to limit the data controller's liability to events where the data controller may have failed to take reasonable steps to ensure compliance by third parties.

Data protection officers and data protection compliance organisations

The Regulation makes it a requirement for a data controller to appoint a data protection officer ('DPO'). This is necessary, and also consistent with global best practices. DPOs are expected to make NITDA's, or the relevant authority's, regulatory role less difficult, since DPOs are better positioned to handle administrative inquiries. The Regulation introduces data protection compliance organisations ('DPCOs') with whom DPOs are expected to closely work. Registered and licensed by NITDA, DPCO's responsibilities include data monitoring and auditing, conducting data protection training, and consulting on data protection compliance. For transparency, the Regulation should have stated the qualification requirements for DPCOs, and the procedure for application. Since DPCOs are independent of NITDA or any relevant DPA, it will be interesting to see how DPCOs carry out their mandate in NITDA's or the relevant DPA's interest.

Establishment of the Panel as an enforcement mechanism

The introduction of the Panel, charged with the responsibility of providing redress to data subjects under the Regulation, is commendable. The Panel is required to:

- investigate allegations of data breach under the Regulation;
- invite affected parties to respond;
- make necessary orders; and
- provide redress all within 28 days.

However, it remains to be seen how the Panel will implement this provision in a country where rights enforcement remains a major challenge, mainly due to a lack of rights awareness, a generally inefficient justice system, weak capacity building, and poor funding. Data breach-related dispute resolution will increasingly become a serious affair in Nigeria, with State and non-state actors. To ensure that the Panel carries out its duties efficiently without fear, favour, or undue influence, its independence should have been secured, and a fund established for its operations.

Beyond establishing a Panel for enforcement of data privacy rights, the Regulation fails to stipulate modern enforcement mechanisms for data protection. In today's technologically advanced world where large-scale data breach is most likely, many data protection regulations now require data processors to implement Privacy by Design principles and carry out periodical Privacy Impact Assessments. These mechanisms boost prevention of data breaches.

Nigeria needs a data protection act, not subsidiary legislation

Nigeria needs a principal legislation on data protection. After the ghostly existence of the NITDA Guidelines for up to six silent years, one would have expected that Nigeria would enact a more comprehensive data protection legislation. For more efficient and effective administration, regulation, and supervision, new legislation should establish an overarching DPA in Nigeria. The establishment of this would not necessarily mean that relevant authorities under the various laws, regulations, and directives would no longer have roles to play in data protection within their sectors and industries, but, by having an overarching DPA, there would be more efficient and effective coordination.

In a GDPR era where every country is putting the power of data back in the hands of its people, I think a more comprehensive data protection regime would have been more appropriate. Particularly in the areas of definite procedures for adequate redress against data breaches, the Regulation is a far cry. While Nigeria may not enact a comprehensive data protection law anytime soon, hopefully all relevant authorities in Nigeria will at least use the Regulation as a general basis for adopting a sector-specific approach to data protection and privacy in their various sectors.

Final words

Though the Regulation does not have all the answers to data protection, by issuing the Regulation less than a year after the GDPR was introduced in the global data protection landscape, Nigeria is demonstrating that it realises how critical the protection of personal data has become in today's data-driven global economy. So, should we be expecting global platforms such as Facebook and Google, for example, to pay as much as NGN 10 million, or 2% of their annual gross revenue of the preceding year, in cases involving more than 10,000 data subjects protected under the Regulation? The answer is **yes** [emphasis added].

In the data game, with both local and global players in an increasingly competitive digital economy where data is 'the new oil,' Nigeria is saying it is ready to play. By the Regulation, Nigeria is taking data protection more seriously. But how NITDA will handle enforcement with other relevant authorities is another kettle of fish.

Senator Iyere Ihenyen Lead Partner
senator@infusionlawyers.com
Infusion Lawyers, Lagos

RELATED CONTENT

NEWS POST

Bulgaria: NRA announces database breach

LEGAL RESEARCH

Recommendation 01/2019 on the Draft List of the European Data Protection Supervisor Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 39(4) of Regulation (EU) 2018/1725) (10 July 2019)

NEWS POST

USA: House Committee passes bills on credit reporting

NEWS POST

Denmark: Datatilsynet issues response to EDPB opinion on Danish draft SCCs

OPINION

Zimbabwe: Emerging legislation on privacy