TEMPLARS

NIGERIA DATA PROTECTION REGULATION 2019:

A SAFETY NET FOR PERSONAL INFORMATION OR JUST BAND-AID?

www.templars-law.com

"Hitherto, the void created by the lack of data protection laws was filled, albeit inadequately by the Constitution of the Federal Republic of Nigeria, 1999 (as amended) (the "Constitution"). Aggrieved persons sought refuge in Section 37 of the Constitution which guarantees the privacy of citizens, their homes, correspondences, telephone conversations and telegraphic materials"

There is growing technological advancement and a continuous shift from manual to digital processes across various sectors globally. This trend has necessitated promulgation of data protection legislation by governments across the world. These legislation are aimed at regulating the collection, collation, storage and processing of personal data by private, public and government entities, as well as safeguarding information of individuals obtained through such digital processes. Nigeria has lagged behind in the development of a regulatory framework for data protection, as there has been a dearth of data protection laws in the country. Hitherto, the void created by the lack of data protection laws was filled, albeit inadequately by the **Constitution of the Federal Republic of Nigeria, 1999 (as amended)** (the **"Constitution"**). Aggrieved persons sought refuge in Section 37 of the Constitution which guarantees the privacy of citizens, their homes, correspondences, telephone conversations and telegraphic materials[1]. In addition, certain sectors (such as telecommunications and banking) have issued specific guidelines and regulations[2] governing data protection.

In light of the foregoing, there was a clamour by various stakeholders for the development of an efficient data protection regime in Nigeria, in line with global standards. In response, on the 25th of January 2019, the National Information Technology Development Agency (**"NITDA"**/ the **"Agency"**)[3] which is the primary regulatory authority responsible for the administration of electronic governance and monitoring of the use of electronic data and other forms of electronic communication transactions[4], issued the Nigerian Data Protection Regulation 2019 (the **"Regulation"**)[5]. The Regulation, which to date[6] is the most comprehensive generally applicable legislation on data protection in Nigeria prescribes the minimum data protection requirement for the collection, storage, processing, management, operation and technical control of personal data[7] in Nigeria.

---

[1] Section 37 of the Constitution of the Federal Republic of Nigeria.
[2] Such as the Nigerian Communications Commission (**"NCC"**) Consumer Code of Practice Regulations 2007, Registration of Telephone Subscribers Regulation 2011 (**"RTSR"**), Central Bank of Nigeria (**"CBN"**) Consumer Protection Framework (**"CPF"**), Regulatory Framework for Bank Verification Number (**"BVN"**) Operations and Watch- List for the Nigerian Banking Industry 2017 (**"BVN Regulatory Framework"**).
[3] The NITDA is established by the National Information Technology Development Agency Act 2007 (the **"Act"**).
[4] Section 6 of the Act.
[5] Section 32 of the Act empowers the NITDA Board to make such regulations as in its opinion are necessary or expedient for giving full effect to the provisions of the Act and for the due administration of its provision.
[6] The NITDA published a ***draft*** Data Protection Guidelines 2017, however, it remained in draft form and was not enforceable.
[7] Personal Data is ***"any information relating to an identified or identifiable natural person* (**"data subject"**); *an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.***

The purpose of this paper is to appraise the capacity of the Regulation to guarantee security of personal information. To this end, this paper will highlight the scope of the Regulation in order to understand its proposed reach in relation to both persons and subject-matter. It will also consider the provisions of the Regulation in relation to security and breach. In addition, this paper assesses the adequacy of the Regulation in securing personal information, in comparison with data protection laws in other jurisdictions. This comparison has intentionally been restricted to African jurisdictions which have enacted data protection laws within the past decade, as a comparison with more developed jurisdictions (such as the United Kingdom ["**UK**"] and Europe) which are arguably pioneers of robust data protection regimes could be adjudged as setting the bar too high. Finally, the effect of the Data Protection Bill (the "**Bill**") in attaining adequate security for personal information in Nigeria will be considered.

SCOPE OF THE REGULATION

The Regulation applies to all transactions intended for the processing of personal data, and the actual processing of personal data in respect of natural persons ***residing in Nigeria or residing outside Nigeria but of Nigerian descent***[8]. It is instructive to note that in outlining its scope, the Regulation does not contemplate protection of entities, as it specifically references only natural persons and not artificial persons. Whilst the intention of the NITDA to protect the personal data of persons of Nigerian descent regardless of their country of residence is laudable, extending the scope of the Regulation to such persons is somewhat overreaching, due to the potential challenges which would be encountered in enforcing the Regulation outside Nigeria. At this juncture, it is important to point out that the Regulation contemplates collaboration with regulatory and law enforcement authorities in other jurisdictions in order to safeguard the privacy of data subjects[9], however the provision in this regard is limited to "***transfer of personal data to a foreign country or an international organization***".

Also, the Regulation is intended to operate as an added layer of protection to existing data protection legislation locally and internationally.[10] Thus, persons who process or control personal data of individuals are also expected to comply with existing obligations in other legislation (as applicable) in addition to those imposed under the Regulation. Furthermore, the Regulation expressly distinguishes between personal data and sensitive personal data[11]. Nonetheless, other than the distinction as contemplated in the respective definitions, the Regulation does not prescribe varying standards in the treatment to be accorded to

[8] Section 1(2) of the Data Protection Regulation.
[9] A Data Subject is "***an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity***".
[10] The Regulation provides that it does not operate to deny any Nigerian or any natural person the privacy rights they are entitled to under any law, regulation, policy, contract, for the time being in force in Nigeria or in any foreign jurisdiction. See Section 1 of the Regulation.
[11] **Sensitive Personal Data** is defined to mean *Data* ***relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.*** *– see Section 1(3) of the Regulation.*

personal data and sensitive personal data. Rather, the Regulation generally requires every data processor[12] or data controller[13] to develop and implement adequate security measures (including deployment of systems/mechanisms to prevent hacking, use of firewalls and use of data encryption technologies) for the protection of data ***"(and other sensitive or confidential data)".***[14] The import of the foregoing is that the Regulation requires the same degree of protection to be accorded to the various components which constitute personal data and sensitive personal data.

It should be noted that, activities which constitute processing as contemplated in the Regulation are ***"any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".***[15]

SECURITY OF DATA AND BREACH OF DATA

Due to the fact that the overarching objective of data protection legislation is ***"guaranteeing security of personal information"***, it goes without saying that adequate security measures and the consequent avoidance of breach should be the fulcrum of any data protection policy/procedure. On this basis, the Regulation provides that personal data should be protected against all conceivable hazards and breaches,[16] such as; theft, cyberattack, viral attack, dissemination, and manipulations of any kind.[17] It further prescribes means of achieving the protection, by requiring anyone involved in data processing or the control of data to develop security measures including; *deployment of systems/mechanisms to prevent hacking, use of firewalls, secure storage of data with restriction of access to specific authorized individuals, use of data encryption technologies, development of organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.*[18]

A data processor or controller will be liable for the actions or inactions of third parties who handle the personal data of data subjects. Thus, it is the responsibility of all data processors or controllers to ensure that the systems of any such third party is of

[12] The Regulation does not expressly define a "data processor" but defines a "data administrator" as ***"a person or organization that processes data"***. Impliedly, a data administrator is a data processor.
[13] A Data Controller as ***"a person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed".***
[14] Regulation 2.6 of the Data Protection Regulation.
[15] Regulation 1.3(r) of the Data Protection Regulation.
[16] The Regulation defines Personal Data Breach as ***"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed".***
[17] Regulation 2.1 (1) (d) of the Data Protection Regulation.
[18] Regulation 2.6 of the Data Protection Regulation.

adequate standard by verifying the integrity of the system. The Regulation also imposes a **general duty of care** towards a data subject on anyone entrusted with the personal data of the data subject or who is in possession of such personal data[19]. Based on the foregoing, as well as the liability of a data processor or controller for the actions or inactions of third parties, the Regulation clearly requires data processors and controllers to act with all reasonable diligence to secure and prevent a breach of data which they process or is in their custody.

ADEQUACY OF SECURITY AND BREACH PREVENTION MEASURES

Taking a cursory look at the security and breach prevention provisions in the Regulation, one might be inclined to take the view that the Regulation provides sufficient security measures for protection of personal data, by virtue of the fact that it contemplates that personal data should be protected against every conceivable form of hazard and breach. Furthermore, it prescribes specific security measures to be taken in furtherance of the required protection. However, further consideration of these provisions in comparison with similar provisions in other African jurisdictions, such as South Africa and Ghana reveals the inadequacy of the provisions under the Regulation.

Like the Regulation, both the South African Protection of Personal Information Act 2013 (**"PPIA"**) and Ghanaian Data Protection Act 2012 (**"GDPA"**) require responsible parties (that is, data controllers/processors) to identify conceivable risk to data and adopt sufficient measures to safeguard data against such risk. However, the PPIA and GDPA go a step further by requiring responsible parties to frequently confirm the effective implementation of the safeguards and ensure the frequent update of such safeguards in response to new risks or deficiencies in previously implemented safeguards. The import of these provisions is that responsible parties have a continuing obligation to ensure proper execution, as well as regular upgrade to guarantee adequacy and efficiency of security measures adopted for the protection of data.

It is instructive to note that the absence of comparable provisions in the Regulation leaves room for ambiguity, as the provisions of the Regulation could be interpreted to mean that the obligation of a responsible party in Nigeria to ensure security of data and prevention of breach is one off. For instance, a company which collects or processes personal information can put measures in place (at the date on which it commences operations) to safeguard the data against all conceivable forms of hazard and breach, and such measures could subsequently be poorly executed or become obsolete, thereby leading to a breach. In such instance, the company may justifiably argue that it is in compliance with extant Nigerian data protection requirements, as there is no provision under the Regulation requiring it to ensure continuous proper execution and/or upgrade of the adopted security measures.

Furthermore, the PPIA and GDPA require responsible parties to notify (as soon as reasonably possible), the applicable regulatory authorities and affected data subject(s) of any unauthorized access to and acquisition of personal data. The notification is aimed amongst others, at providing information to the data subject, to enable such person take proactive protective measures to mitigate the potential

[19] Regulation 2.1 (2) of the Data Protection Regulation.

consequences of the breach. The Regulation does not impose a similar obligation on responsible parties in Nigeria, thus disclosure of a breach is at the discretion of such parties. This creates a leeway for covering up a breach or delaying disclosure, which consequently hampers execution of proactive mitigation measures by the data subject.

It is curious that most data protection laws including the Regulation fail to address mitigating measures upon the occurrence of a breach of personal data. It is observed that even seemingly extensive data protection laws such as the UK Data Protection Act 2018 and the European Union General Data Protection Regulation do not prescribe specific mitigation measures in the event of a breach of personal data. This omission in data protection laws, including the Regulation, is arguably premised on the fact that one of the several purports of data protection laws is the prevention of such breaches. While being mindful of the fact that the principle underlying most data protection laws is precautionary in nature, the law makers will do well to also include comprehensive remedial steps to be taken in the event of a breach. This is in view of the fact that even the most extensive and efficiently enforced data protection laws cannot be foolproof, especially in light of continuous technological advancement and increasing sophistication of cyber criminals.

Despite the shortcomings of the Regulation, the NITDA contemplates the prescription of measures to mitigate a breach of personal data. The draft National Information Systems and Network Security Standards and Guidelines (**"NISNSS"**) provides recommendations for developing an incident response plan for breaches relating to Object Identifiable Information (**"OII"**) which is defined to include; name, address, national identity number and personal identification. The NISNSS requires an organisation affected by an OII data breach to develop a breach response policy and determine whether it should provide individuals affected by the data breach with remedial assistance, such as credit monitoring. Regrettably, these guidelines are currently in draft form and not enforceable until finalized and gazetted.

NIGERIAN DATA PROTECTION BILL: A QUEST TO ATTAIN ADEQUATE SECURITY OF DATA

The Nigerian data protection regime is still a far cry from that of peer African countries. However, the Bill pending before the National Assembly is a viable avenue to address any gaps, omissions or inadequacies in the Regulation. The Bill which is not as extensive as the Regulation, originated in the House of Representatives in 2015. It was transmitted to the Senate in 2017 and is currently at the third stage[20].

The Bill does not include key provisions which are in consonance with international best practice; such as mandatory consent of a data subject to processing, regulation of processing by third parties, appointment of data protection officers by organisations and fundamental considerations in permitting

[20] For clarity, under the Nigerian legislative process, Bills can be originated in either the upper house (the **"Senate"**) or the lower house (the **"House of Representatives"**) of the National Assembly. The Bill will be debated in four stages at the originating house and passed at the end of the fourth stage. Thereafter, the Bill will be transmitted to the other house, debated and passed like in the originating house. Subsequently, the Bill will be sent to the President of the Federal Republic of Nigeria (the **"President"**) for assent and will become a law following the presidential assent.

cross border transfer of data/the yardstick for determining adequate level of protection in foreign countries/territories to which data is transferred. Simply put, the Bill does not provide for security measures to safeguard data and prevent breach.

It is therefore pertinent for the Nigerian legislature to go back to the drawing table and redraft the Bill to include provisions in line with international standards, in order to address the identified loopholes in the Regulation, and foster a robust data protection regime which will ensure security of personal information. That said, any such steps to redraft the Bill should be expedited and the legislature should prioritize the Bill in order to ensure its swift passage. The fact that the Bill is yet to be passed almost four (4) years after its origination, suggests that the legislature is not cognizant of the importance of data protection laws in developing an efficient data protection regime, and the consequential fostering of competitiveness of Nigerian businesses in international trade.

CONCLUSION

The emergence of a generally applicable data protection legislation in Nigeria is most welcome. However, the various drawbacks identified in the Regulation denotes that its advent is unfortunately, not the long awaited safety net for personal information, but a mere band-aid. The Regulation is significant to the extent that it fills the longstanding void in the regime for data protection in Nigeria and mitigates the challenges occasioned by this void. This is a step in the right direction, because there is potential for a more robust data protection regime in Nigeria, provided that there is sufficient commitment to attaining international data protection standards on the part of the legislature[21] and regulators. In this regard, those tasked with the responsibility of lawmaking, as well as the administrators of the data protection regime still have their work cut out for them in developing a data protection regime capable of attaining adequate security of data. It is imperative for the legislature and the NITDA to familiarize themselves with and borrow from similar laws in jurisdictions with efficient data protection regimes in order to swiftly develop extensive and efficient data protection laws capable of providing adequate safeguards for data.

Regardless of its inadequacies, the Regulation would without doubt aid in providing some degree of safety to personal information, consequently fostering competitiveness of Nigerian businesses in international trade and boosting the confidence of individuals in digital processes.

[21] For instance, the National Assembly is yet to enact a Data Protection Act and the Data Protection Bill has been pending before the National Assembly for almost four (4) years.

KEY CONTACTS:

Ijeoma Uju
Partner, Corporate and Commercial

ijeoma.uju@templars-law.com

Adenike Oyeledun
Senior Associate, Corporate and Commercial

adenike.oyeledun@templars-law.com

OFFICE LOCATIONS

Lagos

5th Floor, The Octagon
13A, AJ Marinho Drive
Victoria island
Lagos

Tel: +234 1 46 11 294, +234 1 2703982
+234 1 2799396, +234 1 4611889-90

Fax: +234 1 27 12 810
Email: info@templars-law.com

Abuja

No. 6 Usuma Close
Off Gana Street, Maitama
Abuja

Tel: +234 9 291 1760, +234 9 273 1898
+234 9 273 1877

www.templars-law.com
www.linkedin.com/company/templars
twitter.com/templars_law