The EU GDPR and Nigeria’s NDPR: A comparative analysis

Received: 17th July, 2021

Olumide Babalola
Managing Partner, Olumide Babalola LP, School of Law, University of Reading, United Kingdom

Olumide Babalola, the author of Casebook on Data Protection (Nigeria’s first and only law textbook on data protection), is a prolific and consummate digital rights, consumer rights, and privacy and data protection lawyer. His rich and diverse digital rights litigation experience spans across all superior courts of records in Nigeria and regional courts in Africa, including the ECOWAS Community Court of Justice. He has specifically litigated on privacy and data protection, freedom of information, online freedom of expression and passage of laws protecting digital rights, among others. Olumide has five published books to his credit: the first is a historical piece on the office of the attorney general of the federation and its occupants in Nigeria; the second is a casebook on labour and employment law, which work was propelled by the volume of legal opinions (on Nigerian labour regime, especially the decisions of courts on peculiar issues) he had to write for his multinational company on a regular basis; the third is another casebook on corporate law and practice; the fourth is Babalola’s Law Dictionary, reputed as Nigeria’s first law dictionary (strictly so called); and his latest is a casebook on data protection. He is the managing partner of Olumide Babalola, LP, his flagship full-service law office with a particular bias for digital rights, consumer rights litigation, class actions, and employment and corporate commercial litigation, among others. The awardee of the Nigerian Rising Star Award, he is a member of the Nigerian Bar Association, British Nigeria Law Forum, Internet Society, Internet Governance Forum Support Association (IGFSA), Chartered Institute of Arbitrators (UK), World Litigation Forum, International Bar Association, International Association of Privacy Professionals (IAPP) and International Network of Privacy Law Practitioners (INPLP).

Olumide Babalola LP, Aggey House, 6th Floor, 12 Berkeley Street, Off King George V Road, Moloney, Onikan, Lagos Island, Lagos, Nigeria
Tel: +234 8183645995, +44 7861682348; E-mail: olumide@oblp.org

Abstract It is almost undeniable that the Nigeria Data Protection Regulation (NDPR) derives its inspiration from the European Union General Data Protection Regulation (GDPR). From its title to the contents, the NDPR mirrors its European counterpart in every material respect. Placing both legislation side by side, this paper attempts a comparative review of the similar yet asymmetric regulations. The paper critically analyses the NDPR’s scope, objectives and compliance mechanism vis-à-vis the GDPR’s by interrogating the draftsmen’s intention to arrive at a conclusion on the aptitude of the former.

KEYWORDS: data protection, European Union, GDPR, NDPR, Nigeria, privacy

INTRODUCTION

In 2019, the Federal Government of Nigeria, through one of its agencies, released the Nigeria Data Protection Regulation (NDPR) — a subsidiary legislation — to generally regulate the processing of personal data in the country. A year earlier, the European Union (EU) had commenced enforcing its General Data Protection Regulation (GDPR), which was adopted as the standard for data privacy in all its member states.¹ Some commentators have noted the semblance between this regulation and the GDPR on many fronts.²

This paper critically reviews the areas of similarities and divergence between the two regulations by briefly narrating their origins to appreciate the legislative thoughts and objectives. Comparatively, the paper interrogates the background, scope and
definition of terminologies and concepts as envisaged by similar but distinctive regulations. Using the GDPR as a litmus test, the paper critically compares the entire data protection compliance mechanisms under the NDPR with the European system as envisaged in the former. The paper concludes with suggested reforms to the Nigerian framework.

BACKGROUND
Owing to the need to upgrade the Data Protection Directive 95 to meet the various questions posed by the intrusive advancement in technology, in 2012, the European Commission commenced activities to review the extant directive. The proposal for review was predominantly drafted to harmonise the existing data protection laws within EU member states and to aid free flow of data within and outside the EU with the ultimate objective of guaranteeing personal autonomy over personal data. In December 2015, the European Parliament agreed on the proposal on reforms paving way for the European Council to adopt the GDPR on 8th April, 2016, and afterwards the Parliament signed off on 14th April, 2016, signalling the beginning of a new era in data privacy in Europe and other parts of the world.

Although issued in 2016, the GDPR did not come into force until 25th May, 2018, by virtue of its Article 99 (2), which provides for its enforcement commencement date. The regulation seeks to harmonise the data protection laws of member states in the EU. Hoofnagle et al., however, note that most of its requirements were captured in the Directive 95 albeit with less enforcement and compliance. Dove notes that not only the GDPR is massive, complex and omnibus in its application with 99 articles, 88 pages and 55,000 words, but it also reputed as a well-drafted piece of legislation.

In Nigeria, neither the regulator nor academics have published reports of events leading to the issuance of the Nigeria Data Protection Regulation in 2019. Spurred by the need for Nigerian businesses to measure up to international standards in terms of data protection, the National Information Technology Development Agency (NITDA) invoked its (alleged) powers under section 6(a) and (c) of the NITDA Act to release the NDPR on 25th January, 2019. Prior to the release of the regulation, NITDA had proposed a draft guidelines on data protection in 2013, but the document was never officially issued.

SCOPE OF APPLICATION
Free movement of data within and outside the EU is one of the cardinal objectives of the GDPR, and this underpins its coverage of hybrid data processing and application to entities beyond its immediate jurisdiction. The regulation applies to (automated or manual) the processing of data generally concerning not only European citizens but all individuals within the EU regardless of citizenship. Crutzen et al. conclude that the GDPR cuts a wide net to accommodate all sorts of processing activities within its scope.

The NDPR, on the other hand, also expressly covers all transactions intended for the processing of personal data irrespective of the means of processing. But unlike the GDPR that was issued by the European Parliament, the NDPR is a subsidiary legislation issued by an executive body pursuant to an Act of the Parliament. While the GDPR’s pride of place as an enforceable piece of legislation has not been contended, the same cannot, however, be said of the NDPR, which has questions bordering on legitimacy and weight hovering around it.

Although the NDPR applies to all means of data processing, it is doubtful if NITDA is empowered in its enabling act
to regulate both manual and electronic data.\textsuperscript{16} Section 6(a) and (c), pursuant to which the NDPR was issued, expressly provides for the electronic exchange of information, and it remains doubtful if manual or paper-based personal data can be read into the unambiguous provisions. The Nigerian Supreme Court admonished in \textit{Familonu v. University of Ilorin}\textsuperscript{17} that extraneous words should not be read into clear words in statutes. While it is conceded that preambles are not part of a legislation, they are meant to provide inroads into the draftsman’s intention,\textsuperscript{18} and a cursory look at the NDPR’s preamble will reveal that the regulator is empowered to monitor the use of electronic data as opposed to paper-based methods.\textsuperscript{19}

On its extraterritorial scope, the GDPR contemplates the continued development of international trade, emerging technologies and multistate corporate structures in its application to activities in territories outside the EU.\textsuperscript{20} On one limb, the regulation is applicable to processing ‘in the context of activities of an establishment of a controller or processor in the union, regardless of whether the processing takes place in the union or not’.\textsuperscript{21} Here, the GDPR will still apply to an entity even if it is domiciled outside the EU, where its processing is in the context of activities of an establishment within the region and for the avoidance of doubt. Moerel notes that this principle has a virtual nature but binds a controller even when not physically within the EU.\textsuperscript{22}

The NDPR extends its application to Nigerian residents within and outside Nigeria, but unlike under the GDPR, where the extraterritorial application is qualified, the NDPR does not set any parameters for its extraterritorial application. That makes it difficult or impossible to enforce the regulation outside the shores of Nigeria. Even the EU’s layered approach to extraterritoriality of data privacy laws has been branded ‘unsophisticated’; hence, one wonders how the NDPR seeks to paddle its extraterritorial canoe.\textsuperscript{23} The NDPR Implementation Framework issued in November 2020 does not also offer the needed clarity on the working of NDPR’s extraterritoriality; hence, it is left to conjecture.\textsuperscript{24} It is conceded that extraterritorial possibilities cannot be wished away from data protection laws, otherwise adequate protection would not be offered; the modalities for enforcement, however, must be realistic and well articulated in the light of issues surrounding conflict of laws.\textsuperscript{25}

Kuner et al. identify extraterritoriality as a common trend with data privacy laws, citing examples in Singapore and Malaysia. A perusal of the pieces of legislation, however, reveals some sort of legislative justification or guide that is absent in the NDPR.\textsuperscript{26} Like the GDPR, NDPR’s extraterritorial proposition is bereft of any institutional framework or guidelines as to its enforcement. Researchers have noted that the most prominent drawbacks of extraterritorial provisions in privacy and data protection laws are the insufficiency or impracticability of their enforcement drives.\textsuperscript{27}

Ultimately, it is believed that the NDPR’s proposed application to citizens resident outside Nigeria without clear guidance notes from the supervisory authority (SA) on its mechanisms is, in the words of Svantesson, ‘meaningless, useless and at the same time causes confusion and hinders constructive debate’.\textsuperscript{28} Ultimately, apart from the anonymised data, the GDPR also exempts its application from processing data for purely personal or household use, and/or in the context of national security,\textsuperscript{29} but the NDPR contains no such legislation.

**DEFINITIONS OF TERMINOLOGIES AND CONCEPTS**

The GDPR and NDPR share similarities in their definitions of some concepts but with slight variations here and there. Both regulations are almost the same with
their identical definitions of personal data, processing, filing system, data controller, third party, consent, personal data breach and recipient.\textsuperscript{30} The NDPR, however, defines data, data portability, sensitive data and foreign country, but these terms are not defined in the GDPR, which, however, defines restriction of processing, profiling, pseudonymisation, generic data, biometric data, data concerning health, main establishment, enterprise, binding corporate rules, SA, cross-border processing, information society service and international organisation. Those terms are not explained in the NDPR.\textsuperscript{31}

**Data administrator**

While the GDPR defines a data processor as an entity that processes data on behalf of a controller, the NDPR introduces a rather confusing concept of ‘data administrator’ and identifies it as an entity that simply processes data. To put this in proper context, data administration has been described as ‘consisting of data analysis and functional analysis to yield a conceptual data model and then corresponding conceptional process model for an organization’.\textsuperscript{32} In identifying the traditional functions of data administrators (DAs), Fry notes that the concept has been around since the early seventies when researchers had conceptualised the role in terms of its functions and duties in an organisation.\textsuperscript{33}

Hasegawa and Nishio note that as opposed to a database administrator (DBA) that implements designs and maintains database, DAs are expected to introduce and control methodology and procedure for storage, management and grouping of data (not necessarily personal data) from an organisational point of view.\textsuperscript{34} Contrary to the definition and job description assigned them under the NDPR, the traditional role of DAs is to ensure that databases run efficiently.\textsuperscript{35} The NDPR conflates ‘processor’ with DA, but going by the literal definition of DA thereunder, it appears everyone that processes data (ie controllers, processors, third parties, recipients) in the data protection ecosystem is erroneously contemplated within the definition. This could not have been the intention of the draftsmen, as, within the context of data protection, what differentiates data processor from controller is the contractual engagement of the former to carry out processing activities on behalf of the latter.\textsuperscript{36} The unwarranted introduction of the term or its seeming conflation with ‘data processor’ in the NDPR was, however, technically confirmed by its conspicuous omission in the body of the regulation where the term ‘data processor’ is intended.\textsuperscript{37}

**Sensitive data and special category of personal data**

In spite of the GDPR’s undisputable consideration as an international standard for data protection laws in the world, it is not without its own inherent failings.\textsuperscript{38} The GDPR places a high premium on sensitive data (special categories of personal data) by allowing member states to set parameters for processing ‘special categories of personal data’ in relation to fundamental rights and freedoms, but surprisingly nowhere in the regulation is sensitive data defined, other than prohibition of processing without seeking (special) consent with exceptions.\textsuperscript{39} Rather than define the term, the regulation in its context-based approach leaves the meaning open ended to include all personal data that are by their nature sensitive in relation to fundamental human rights.\textsuperscript{40}

Researchers have, however, justified the GDPR’s approach as it encompasses both data and its processing in the consideration of its sensitivity or otherwise.\textsuperscript{41} However, the NDPR defines sensitive data to mean all data relating to religious beliefs, sexual orientation, health, race,
ethnicity, political view, trade union membership, criminal records and other sensitive personal information. Like the GDPR’s grouping of sensitive data, this definition is also open ended especially with the inclusion of the phrase ‘other sensitive personal information’. Although the NDPR does not tie the sensitive personal data to fundamental human rights, the empirical meaning of sensitive information as used in its relevant provision suggests a wide net of inclusivity, for instance, financial data is not expressly listed but it can be accommodated under ‘other sensitive personal information’.

**Personal identifiable information**

Any information that can be used (on its own or with other information) to identify a data subject is personal identification information (PII) under the NDPR. Conversely, the GDPR neither defines nor makes reference to PII, but it remains to be seen how the definition of personal data thereunder can be distinguished from the definition of PII under the NDPR. Personal data (PD) and PII are similar and equivalent concepts that are adopted by jurisdictions exclusive of each other; hence, the concept of PII is already covered under PD and the former’s presence in the regulation is otiose and serves no practical purpose.

**Anonymisation and pseudonymisation**

In its risk-based approach, the GDPR defines pseudonymisation of data, especially where sensitive data is processed and excludes its application from anonymous data as described. Other than defining sensitive data, the NDPR neither contemplates pseudonymisation nor makes an exception for anonymised data, unlike the GDPR, which encourages pseudonymisation as a data security and confidentiality measure.

**PRINCIPLES OF DATA PROTECTION**

Taking a cue from the repealed Directive 95, albeit with a slightly different nomenclature and addition, the GDPR lists seven principles of European data protection law to wit: lawfulness, fairness and transparency, data minimisation, purpose limitation, storage limitation, accuracy, integrity and confidentiality and the newly introduced accountability principle.

The legislative style adopted under the NDPR makes it a bit difficult to ascertain the number of principles provided under the regulation. The principles appear muddled up in an indecipherable manner; it, however, can be argued that regulation 2.1 thereof provides for the following: lawfulness (in the absence of fairness and transparency), accuracy, purpose limitation, storage limitation, integrity and accountability. The omission or some principles appears one of the ills of legal transplantation plaguing the Nigerian legal system that encourages replication of foreign laws without considering the country’s peculiar local circumstances.

Unlike the GDPR where the principles are separated and particularised, the NDPR does not identify the principles individually; hence, it is not only problematic to ascertain whether the principles are five or six, but their comparability with the European principles also appears questionable.

**LEGITIMATE INTEREST**

The GDPR, in a clear manner, lists the grounds that constitute lawful processing of personal data, including ‘legitimate interest pursued by the controller or a third party’ as one of them. This ground is also referred to as the ‘balance of interest’ provision. It has also been considered as the go-to provision that provides an ever-ready alternative to data controllers when other legal bases become unattainable. It simply means that processing of data under this limb
must be necessary for the legitimate business of the controller or a third party.54

This ground of lawful processing is, however, conspicuously missing under the NDPR, and this puts most controllers at risk of violating data subjects’ rights, especially where other grounds are impracticable. Again, in a bid to salvage the situation, the Nigeria DPA included legitimate interest as a ground in the implementation framework for NDPR, such inclusion faces a legitimacy test on its own especially as it is not supported by any provision in the extent regulation which it is meant to clarify.55

DATA SUBJECTS’ RIGHTS

The NDPR, like GDPR, recognises data subjects’ rights: (a) to be informed on processing activities on their data in a concise and intelligible manner; (b) data subjects’ request of access to personal data; (c) rectification of personal data; (d) erasure/deletion of personal data; (e) restriction of processing; (f) data portability; (g) withdrawal of consent; (h) lodge complaint with an SA; (i) information on automated decision making; (j) information on international transfers; (k) objection to processing; (l) restriction on processing.56

Some slight disparities, however, exist in both regulations’ provisions of data subject rights: unlike the GDPR, the NDPR does not provide exceptions or qualifications to the exercise of the right of erasure. Again, the Nigerian regulation does not make any reference to indirect collection of personal data in relation to the right to be informed, unlike the GDPR, which mandates controllers to inform data subjects within one month of collection.57 While under the GDPR data subjects can still object to processing even where done in the public interest, they cannot rely on the NDPR to make such objection.58 With respect to data subjects’ access to personal data, the NDPR does not specify the information that must be provided by controllers in response to the requests, unlike the GDPR. The latter lists the categories of information that must be given to a data subject in the event of access request.59 The exercise of the right of access is limited by the fundamental rights of others under the GDPR, but no such derogation exists under the NDPR.

While time can be extended under the GDPR for the provision of access to personal data, no such extension is contemplated under the NDPR.60 The NDPR does not provide for a right not to be subjected to automated decision making but such exists under the GDPR.61 The NDPR rather contemplates that a data subject must be informed of the existence of automated decision making.62 In exercising the right to data portability, the GDPR provides the right to receive data in a structured, commonly used machine-readable format, which is replicated by the NDPR. However, both regulations do not provide much clarity on the workability of the identical.63

Another striking difference between the provisions of both regulations on data subjects’ rights is that, unlike the NDPR, the GDPR envisages that such rights must correspond with fundamental rights.64 This undoubtedly informed judicial decisions on the enforcement of data protection rights in Europe.65 Conversely, the Nigerian Federal High Court in Laws & Rights Awareness Initiative v. National Identity Management Commission did not see any correlation between data subjects’ rights provided under the NDPR and fundamental rights provided under Chapter 4 of the Nigerian Constitution.66

CHILDREN’S DATA

Both regulations oblige controllers to take proactive steps in providing information to children (data subjects) in a concise, transparent, intelligible and accessible form using a clear and plain language that the child can easily understand.67 Whereas the GDPR makes specific and comprehensive
provisions on data controllers’ obligations when dealing with children’s data, affording protection for their vulnerabilities as well as provisions on parental consent, the NDPR is silent on these.68

While the GDPR sets 16 years and not below 13 years for member states as the threshold for the age of a child to seek consent for personal data processing,69 the NDPR’s omission of consent age throws up a lot of questions considering conflicting statutory provisions on definition of a child in Nigeria.70

DATA PROTECTION OFFICER

Whereas the GDPR only requires data controllers to designate data protection officer (DPO) in certain specific circumstances, such as public bodies, surveillance businesses or businesses, that involve large-scale sensitive data processing, the NDPR requires all data controllers to designate DPOs without exception.71

Again, the GDPR makes copious provisions on qualities, roles, competence, expectations and tasks of the DPO but the NDPR merely saddles him or her to ensure adherence to the regulation without more definition. That thereby leaves the question of qualification, responsibilities and status of a DPO to conjecture. Unlike under the GDPR, it is arguable if issues of conflict of interest can arise between a Nigerian DPO and his organisation with the current state of the NDPR.72 It is worthy of note that the Implementation Framework 2020 issued pursuant to the NDPR appears to have widened the scope, but it is arguable whether such a guidance note can technically amend the provision of the regulation to plug regulatory gaps.73

DATA PROTECTION COMPLIANCE ORGANISATION

The NDPR undeniably scores a first with its introduction and styling of Data Protection Compliance Organisations (DPCOs) as an enforcement and compliance agent in Nigeria’s data protection system.74 A DPCO is defined as an entity duly licensed by NITDA for training, auditing, consulting and rendering services and products for compliance with the NDPR or any foreign data protection law or regulation affecting Nigeria.75 They are predominantly licensed by the Nigerian DPA and another player in the compliance system to ease the burden of enforcement and compliance.

As much as the appellation of DPCO appears unique to NDPR, the GDPR also makes provision for a similar body with an appropriate level of expertise that could be accredited by SAs to monitor compliance.76 Silberman and Johnston note that the certification of ‘monitoring bodies’ will help address issues of enforcement and standardisation in self-regulation.77

DATA PROTECTION AUDIT

This is a key feature of the Nigerian data protection compliance mechanism which mandates data controllers to file an annual data protection audit with the SA by stating certain information including: disclosing the legal basis(es) for processing, transparency and data protection policies of such controller, data security measures, contact of data protection officer (if any) etc.78 Although controllers are meant to conduct self-audit within six months of issuance of the regulation, the annual audit is usually carried out by DPCOs on behalf of the SA, on data controllers that are above the threshold of 2000 data subjects79 even though neither the regulation nor its implementation framework provides parameters for detection of the number of data subjects, especially as website visitors are also contemplated in this group of data subjects for data protection purposes.80

Under the GDPR’s self-regulatory and co-regulatory regimes, DPOs play a role in related audits and a group of undertakings
is also required to set up mechanisms for data protection audits and methods for corrective actions to protect the rights of data subjects. Gleeson and Walden have, however, argued that under European law, evaluative standards ought to require data protection audits conducted by third parties (as found in the NDPR). Ultimately, SAs can also carry out investigations in the form of audits rather than as routine annual activities obtainable under the NDPR. Some EU member states, however, have enacted laws obliging SAs to audit controllers both as a routine and part of investigatory activities.

INTERNATIONAL PERSONAL DATA TRANSFER

Both the GDPR and NDPR provide similar conditions for the international transfer of data. The area of divergence, however, is in ‘transfers on the basis of adequacy decisions’, where decisions are made by the European Commission, upon consideration of the factors provided in Article 45(2) under the European regulation but in Nigeria, it is the SA or the Nigerian Attorney General of the Federation that makes adequacy decisions under the NDPR.

One of the major concerns addressed by the GDPR is the increased risks of privacy violations exacerbated by transborder data flows that enhance misuse and compromise of personal data for purposes other than its agreed use. Under the GDPR, the European Commission’s decision may be made by an implementing act subject to review every four years but the NDPR is silent on how the adequacy decisions are made or reviewed. Researchers have noted that the lack of definition for ‘international personal data transfer’ in the GDPR has decided what constitutes such transfers more difficult.

As an exception to the adequacy level requirement for international transfer of data, the GDPR also allows such transfers to be made where appropriate safeguards like enforceable instruments between public bodies, binding corporate rules, standard data protection clauses and approval codes of conduct. The NDPR, however, does not make provision on the appropriate safeguards in the absence of an adequate decision, but it provides grounds upon which transfers can take place.

DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment (DPIA) has been described as a ‘systematic process to investigate, identify and minimise risks in a project or big data platform for the protection of personal data’. The obligation to conduct DPIA is only activated under the GDPR where a controller employs new technologies to process personal data and is likely to result in high risks to fundamental rights and freedoms.

The NDPR does not expressly require controllers to conduct DPIA but mandates them to set up policies and procedures for assessing the impact of technologies on privacy. It can be, however, argued that the NDPR contemplates Privacy Impact Assessment (PIA) defined as a process that a data controller evaluates and considers the privacy risks of new methods of processing personal data. Researchers have, however, argued that PIA, although related, is distinguishable from DPIA that operates with fundamentally different tools and requirements. From the provision of the NDPR, it appears that a controller may merely draft policies and still be compliant without necessarily conducting DPIA where necessary.

DATA BREACH NOTIFICATION

O’Brien notes that the GDPR introduced an EU-wide data breach notification into European data protection law. Recital 85 and Article 23 require a controller and
The EU GDPR and Nigeria’s NDPR: A comparative analysis

processor to notify the relevant supervisory activity within 72 hours of its discovery of the personal breach. Controllers are also duty bound to inform data subjects of data breaches in certain circumstances, and in the event of any delay in notifying the SA, they must furnish an explanation.98

The NDPR neither provides for notification of the SAs nor the data subjects in the event of personal data breach, but the implementation framework, however, provides for notification under clause 9.0 thereof.

ADMINISTRATIVE REDRESS PANEL

As part of its enforcement mechanism, the NDPR introduced the Administrative Redress Panel (ARP) to investigate allegations of violation of data subjects’ rights and to determine appropriate redress and administrative orders.99 The GDPR does not contemplate any administrative panel rather, certain boards are created thereunder. The European Data Protection Board (EDPB) is established to issue guidelines to SAs among other functions.100 Additionally, SAs under the GDPR are saddled with the task of investigating and handling complaints of violations of the GDPR.101

ENFORCEMENT AND ADMINISTRATIVE FINES

Co-regulatory and self-regulatory is a hybrid approach adopted by the GDPR to ensure compliance and enforcement of data subjects’ rights.102 The regulation introduces legislative and self-regulatory activities such as certifications and technical standards to ensure controllers’ alignment with certain standards.103 Here, SAs within member states are empowered to establish certification mechanisms to depict controllers’ levels or standards of compliance with the GDPR.104 In the event of a violation, the GDPR empowers SAs to issue administrative fines ranging from €10m to €20m or between 2 per cent and 4 per cent of defaulting controller’s global annual revenue for the last financial year, whichever is higher.105

In a similar fashion and as a consequence of breach of data subjects’ rights, the NDPR imposes a fine of ₦2m or 1 per cent of annual gross revenue for controllers with less than 10,000 data subjects and a fine of ₦10m or 2 per cent of the annual gross revenue of the preceding year for controllers with more than 10,000 data subjects.106 Unlike the GDPR that provides factors that must be considered by the SAs before imposing appropriate fines, the NDPR does not provide any guidance on the parameters of sanction.107 The GDPR expressly clarifies the nature of time issued by SAs as administrative but the NDPR appears to have given a rather confusing impression with the phrase ‘in addition to any other criminal liability’ giving way to arguments that the fine contemplated thereunder is quasi-criminal in nature.108

SUPERVISORY AUTHORITIES

An SA is an independent public authority established by an EU member state to be responsible for monitoring compliance with the GDPR.109 SA is also referred to as data protection authority (DPA).110 The GDPR empowers member states to establish independent bodies to act as SAs as well as the general conditions of appointment to guarantee impartiality and competence.111 In Nigeria, compliance with data protection regulation is supervised and monitored by the ARP, the Attorney General of the Federation (HAGF) and NITDA under the NDPR.112

Although the term ‘supervisory authority’ appears once in the regulation, it is not clear as to which of the bodies was referenced. Rhiannon et al. note that the ARP and HAGF are granted supervisory powers under the NDPR without reference to NITDA; hence, it is doubtful which of the entities reserves the exclusive powers
of an SA under the Nigerian regulation when the conflicting provisions are read together. \(^{113}\) This confusion is further compounded by the definition of ‘relevant authorities’ to include any other statutory body or establishment having government’s mandate to deal solely or partly with matters relating to personal data. \(^{114}\) The expansive definition accommodates public bodies such as Central Bank of Nigeria, National Identity Management Commission, Nigerian Communications Commission, Nigerian Immigration Service and other government agencies that process personal data. Invariably, there is hardly any government agency that does not deal with data.

A fundamental omission in the NDPR concerns independence and impartiality of the SA, which is a defining feature of Data Protection Authorities. \(^{115}\) The NDPR is silent on establishment, appointment of officers, budgeting removal and other factors that guarantee independence, impartiality and competence of SAs. Although NITDA has been severally referred to as Nigeria’s SA, not only does the NDPR omit an express provision on that, researchers have also argued that NITDA lacks the statutory powers to regulate data protection in Nigeria. \(^{116}\)

**REDRESS MECHANISM**

One of the major perceived obstacles to the success of the NDPR has been its enforcement in the courts of law. Whereas the GDPR empowers data subjects to seek compensation for violation of the regulation either personally or through a not-for-profit organisation, the NDPR does not have such progressive provisions. \(^{117}\) As a result of this far-reaching omission, the Nigerian Federal High Court ruled in *Digital Rights Lawyers Initiative (DRLI) v. Unity Bank Plc* \(^{118}\) that only a data subject can file an action for data breach and that, not-for-profit organisations cannot file on their behalf. In that case, the personal data of over 50,000 job seekers were exposed on the respondent bank’s job portal and the applicant, a nongovernmental organisation (NGO) approached the court for declaratory reliefs, but the court dismissed the suit for lack of locus standi on the part of the NGO. In an earlier case of *Digital Rights Lawyers Initiative & 2 Ors. V. National Identity Management Commission*, \(^{119}\) the Applicants contended that right to rectification ought to be exercised free of charge but the court held that such right was not contemplated under the fundamental right to privacy.

In another case between DRLI and LT Solutions Multimedia Limited \(^{120}\) where a data broker was sued for selling data subjects’ personal data without legal basis, the High Court of Ogun State declined jurisdiction to compel NITDA to sanction the respondent but held, that NDPR is quasi-criminal legislation, and its violation can only be redressed by criminal prosecution at the Federal High Court rather than the States’ High Court. The most recent decision on the NDPR was delivered by the Federal High Court sitting in Ibadan where DRLI sued the National Youth Service Corps for the publication of corps members personal data in a magazine without valid consent as required under regulation 2.3 of the NDPR even though the corps members signed a consent form on the eve of their passing out parade. The applicant argued in that case that such consent was not ‘freely given’ as contemplated by regulation 1.3(iii) of NDPR. In dismissing the suit, the court noted that as the consent form had a clause for withdrawal of such consent, it fulfilled the requirements of the NDPR in that respect.

Since its issuance in 2019, court decisions on the NDPR have been very few \(^{121}\) and unhelpful in the development of the field, especially as the Nigerian courts are yet undecided on whether to treat data protection as a component of the fundamental right to privacy or a civil cause of action ordinary civil cause of action
thereby making the proper procedure for
litigating the concept unsettled. This has
greatly hampered public interest litigation
on data breaches unlike under the GDPR
where data subjects can mandate not-for-
profit organisations to exercise the available
rights on their behalf.

CROSS-BORDER COOPERATION
It has been repeatedly noted that the
GDPR was introduced to harmonise data
protection laws and regulations around
Europe. To achieve this objective, the
European Commission and the SAs within
the EU are obliged to develop international
cooperation mechanisms to protect personal
data especially when transferred to third
countries. Deursen et al. note that these
mechanisms are expected to introduce
formidable protection and enforcement
measures for data subjects’ rights.

The NDPR also replicates this provision;
it, however, looks like a domestic
arrangement rather than the international
coooperation envisaged under the GDPR,
where the SAs of the various member states
are to develop international cooperation
mechanisms. Under the NDPR, NITDA —
a Nigerian agency is to work with ‘relevant
agencies’ — other Nigerian agencies — to
develop (international) mechanisms.

Nevertheless, it has been suggested that
NITDA can rely on this provision to take
advantage of the ECOWAS Supplementary
Act on Personal Data Protection or
other international instruments to forge
international cooperation with member
states within the ECOWAS subregion
to kick start the instrumentation of the
provision.

CONCLUSION
Moving on from Nigeria’s failed legislative
attempts at regulating data privacy since
its return to democratic government, its
reliance on the GDPR to release the first
general regulation on the subject is not an
entirely bad way to start, notwithstanding
the inadequacies and what appears a legal
transplantation in this context. This paper
has examined the NDPR’s simulation of
some European data protection concepts
with a blend of some American terms
in a manner that poses the question of
consistency. The paper has analysed the
GDPR’s standards vis-à-vis the NDPR’s
omissions of concepts, mechanisms with
instructive guidance and its implication on
the Nigerian data protection legal system
citing examples of decided cases exposing
the effect of the regulatory inconsistencies
on court decisions worsened the absence of
local judicial precedents on the subject.

Conclusively, it is conceded that
the NDPR thankfully opened an
unprecedented vista in Nigeria’s data
protection ecosystem and effectively placed
data privacy issues on the front burner
within and outside her courtrooms like
never before. Having ostensibly taken its
inspiration from European models and
standards, the NDPR surprisingly left so
many questions unanswered, which posers
cannot be catered to by guidance notes or
implementation frameworks, but proper
quasi-legislative or legislative intervention
is for complete review of the regulation or
an enactment of a principal data protection
legislation that will not only adequately
and comprehensively plug the regulatory
gaps but also contextualise the country’s
sociopolitical with statutory realities in the
light of its provisions.

Nigeria’s significant reliance on the
GDPR to release her first general legislation
on data protection is not an entirely bad way
to start, notwithstanding the inadequacies
and confusion of some concepts. This paper
has examined the NDPR’s simulation of
some European data protection concepts
with a blend of some American terms,
in a manner that poses the question of
consistency. The paper has analysed the
GDPR’s standards vis-à-vis the NDPR’s
omissions of concepts, mechanisms with instructive guidance and its implication on the Nigerian data protection legal system, citing examples of decided cases that expose the effect of the regulatory inconsistencies in the NDPR on the courts’ decisions. This is worsened by the absence of appellate judicial precedents on the subject matter.

Nevertheless, having ostensibly taken its inspiration from European models and standards, the NDPR left so many questions unanswered, which cannot be catered to by guidance notes or implementation frameworks, but by proper quasi-legislative or legislative intervention. A complete review of the NDPR or an enactment of a principal data protection legislation will not only adequately and comprehensively plug the regulatory gaps identified in this paper, but will contextualise the country’s sociopolitical peculiarities with statutory realities in the light of its provisions. For example, very important terms like ‘child’, ‘age of consent’ and supervisory ‘authority’ must be defined, and clarification is needed on the preferred procedural approach for data breaches as well as a definitive position on the imposition of fines as criminal sanctions or administrative penalties.

References and Notes


9. Stakeholders have speculated whether the NITDA Act empowers the public body to generally regulate personal data; no court decision, however, exists to the contrary.


12. General Data Protection Regulation, art. 2(1). See also Crutzen, I. Ragman Peter, G.-J. and Mondschein, C. (2019) ‘Why and how we should care about the

13. NDPR, Reg. 1.2(a).

14. National Information Technology Development Agency Act 2007, section 6(a) and (c).


16. NDPR, Reg. 1.2(a), ref. 13 above.

17. (2017) 2 NWLR (Pt. 1017) 74.


19. ‘WHEREAS, The National Information Technology Development Agency (NITDA, hereinafter referred to as The Agency) is statutorily mandated by the NITDA Act of 2007 to, inter alia; develop regulations 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’.


21. GDPR, art 3(1). A similar provision under the Directive 95 has been interpreted by the CJEU to enhance the extraterritorial grip of the legislation in Weltimmo’s case. See Babalola, O. (2020) ‘Casebook on data protection’, Amazon, p. 424.


29. See art 2(2)(c) and (d) for the exemptions.

30. GDPR, art. 4, NDPR, Reg. 1.3.

31. Ibid., art 4.


37. NDPR, Regs. 2.4(b) and 4.1(3).


40. GDPR, recs. 10, 51, 54, 71 and 91, art. 9(1).

42. Reg. 1.3 (xxv).
44. Reg. 1.3(xx).
52. Recs. 47, Art. 6(1)(f).
55. Clause 2 of the framework makes it clear that its purpose is provision of clarity to the NDPR and that it does not supersede the regulation. Hence, it cannot import legitimate interest into it through the backdoor.
56. NDPR, Reg. 2.5, 3.1, GDPR, art. 12–23.
58. GDPR, art. 21(1).
59. Ibid., art. 15(1).
60. Ibid., art. 12(5).
61. Ibid., art. 22(1).
62. NDPR, Reg 3.1(7).
63. GDPR, recs 60, 68, article 20; NDPR, Reg 3.1(14).
66. (Unreported) Suit No. FHC/AB/CS/19/2020 delivered by I. Watila, J sitting in Abeokuta, Ogun State.
71. GDPR, art. 37, NDPR, Reg. 4.1(2).
The EU GDPR and Nigeria's NDPR: A comparative analysis


74. Babalola, ref. 10, above, p. 4.

75. NDPR, Reg 1.3(xiii).

76. See GDPR, art 41(1).


78. NDPR, Reg 4.1 (5).

79. Ibid., Reg 4.1(6).


83. GDPR, art. 58(1)(b).


85. Reg 2.11 and 2.12.


90. Reg. 2.12 simply allows international transfer of data where any of the lawful bases exist.


93. Ibid., Reg 4.5(j).


99. Ibid., Reg 4.2.

100. Ibid., rec. 72, art. 68.


106. Ibid., Reg 2.10.

108. This argument was canvassed by Counsel to Truecaller in the pending Suit No. FHC/ABJ/CS/1432/19 between Olumide Babalola LP and True Software Scandinavia AB before the Federal High Court sitting in Abuja and also alluded to in a judgment by the High Court of Ogun State in (Unreported) Suit no. HCT/262/2020, per Ogunfowora, J.

109. Ibid., art. 51(1).


112. Ibid., Reg. 2.11, 4.2(2).

113. Gibbs-Harris, ref. 67 above.

114. Ibid., Reg. 1.3(xxv).


119. Unreported) Suit No. AB/83/2020 delivered by High Court of Ogun State per A. A. Akinyemi, J. on 15th July, 2020, and it is subject of appeal number CA/IB/291/2020 at the Ibadan division of the Court of Appeal.

120. (Unreported) suit No. HCT/262 delivered on 9th November, 2021.

121. Only about five decisions have been delivered by the high courts, but there are no appellate court decisions on the regulation yet.


124. Ibid., art. 50 (a)–(d).


126. Ibid., Reg. 4.1.