AO2LAW
Anaje · Olumide · Oke · Akinkugbe

AFFIXING THE NATIONAL IDENTITY NUMBER ON COURT PROCESSES: THE NIGERIA DATA PROTECTION REGULATIONS 2019 IN PERSPECTIVE

Introduction

The Nigeria Data Protection Regulations 2019 (the **"NDPR"**) was enacted pursuant to the National Information Technology Development Agency (**"NITDA"**) Act of 2007 (the **"Act"**) to provide safeguards on privacy and protection of Personal Data of persons in Nigeria and all Nigerians around the world. Since the inception of the NDPR, the Regulatory body, NITDA, has taken steps to ensure compliance with same by amongst others, mandating organizations in Nigeria who have access to the Personal Information of 1,000 (One Thousand) Data Subjects or more to conduct audits for this purpose and subsequently file audit reports with NITDA.

The "Mandatory Use of National Identification Number Regulations of 2017" (the **"NIN Regulations"**) made pursuant to the National Identity Management Commission Act, 2007 (the **"NIMC Act"**), compels the use of National Identification Number (NIN) when filing and registering criminal and civil actions in courts or in arbitration processes.

This briefing note seeks to examine the interplay between the NIN Regulations, the NDPR and the general impact on data protection in Nigeria.

Definitions of Key Terms:

Breach — 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;

Data Controller — A person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed;

Data Subject — Any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Personal Data — Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context;

Sensitive Personal Data	Data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information

Relevant Legal Provisions

The key legal provisions to consider include the following:

A. **Regulation 1 (1) (u) of the NIN Regulations** provides as follows:

"(1) In accordance with the provisions of section 27 (1) (1) of the Act, the use of the National Identification Number (NIN) shall be mandatory for the following additional transactions-

(u) filing and registration of criminal and civil actions in courts or other arbitration processes;

B. The NDPR 2019, whose relevant provisions shall be discussed in detail in succeeding paragraphs is aimed towards safeguarding rights of natural persons to data privacy amongst other things.

The NIN Regulations and the Protection of Data Subjects

The NIN Regulations derive its legal basis from Section 27 of the NIMC Act and compels the use of NIN for filing of court and arbitration processes. The Nigerian Judiciary has since had the opportunity to review the provisions of the NIMC Act and NIN Regulations and determine their relevance or otherwise, albeit without considering the provisions of the NDPR. The Court in *SLB Consortium Limited v. NNPC* (2011) 9 NWLR 317 held that for a court process to be duly endorsed under Nigerian law, it must have the name of a legal practitioner and where there are multiple lawyers, the name of the lawyer signing must be indicated. The lawyer must also state the name of the law firm he/she is practicing with (if any), address for service, telephone number, National Identification Number and an email address registered with the Nigerian Bar Association.

Under the NDPR (specifically Regulation 2.2(c)), one of the lawful basis of data processing is that it complies with a legal obligation to which a Data Controller is bound. The NIN Regulations impose an obligation on courts and arbitration panels/institutions to ensure that NINs are required for the filing of processes, therefore the collection of NINs by courts or arbitration panels/institutions does not in any way violate the lawful basis of data processing as contained in the NDPR.

Notwithstanding the foregoing, the NIN Regulations raise a few concerns from a data protection perspective especially with regards to security of personal data and compliance with the provisions of the NDPR by courts and arbitration panels/institutions in general. Under the NDPR, anyone involved in data processing or the control of data shall develop security measures to protect data (please see Paragraph 2.6). Bearing in mind that NINs would qualify as Sensitive Personal Data under the NDPR, a higher level of responsibility is

required by Data Controllers such as the courts and arbitration panels with regards to securing such Personal Data. The question that comes to our mind is – Do courts/arbitration institutions have sufficient security infrastructure to protect Sensitive Personal Data such as NINs?

Our response to this question is that the courts need to pay more attention to the security of Personal Data in its possession bearing in mind the high possibility of a data breach considering the current mode of storage of Personal Data by Nigerian courts. It is necessary to mention that Data Controllers such as the courts and arbitration panels/institutions are subject to the provisions of the NDPR with regards to data security and have a potential exposure to sanctions under the NDPR. Therefore, the courts and arbitration institutions must ensure that appropriate risk mitigation strategies are adopted. This is particularly relevant considering that government agencies including the judiciary are subject to the provisions of the NDPR. As we have seen in recent times, the NITDA has launched investigations into alleged incidents of breach by a government agency which shows that government agencies are not immune to sanctions in the event of personal data breach. Therefore, in our view it is necessary that the relevant safeguards with regards to Personal Data Protection are put in place. This is particularly important in view of the provisions of the NDPR. For example, Paragraphs 2.1(2) and (3) of the NDPR provides that:

> *"(2) Anyone who is entrusted with the Personal Data of a Data Subject owes a duty of care to the said Data Subject;*
> *(3) Anyone who is entrusted with Personal Data of a Data subject or who is in possession of the Personal Data of a Data subject shall be accountable for his acts and omissions in respect of Data processing, in accordance with the principles contained in this regulation."*

In addition, another important compliance requirement under the NDPR is the privacy policy obligation. Under the NDPR, there is the requirement for Data Controllers to display a simple and conspicuous privacy policy that the class of Data Subjects being targeted can understand. Irrespective of whether NINs are part of court and arbitration processes or not, it is necessary courts and arbitration institutions include relevant privacy notices at the point of filing (perhaps at the relevant registry) detailing the purposes for collection of Personal Data and other information stated in Paragraph 2.5 of the NDPR.

Conclusion:

A key principle of Data Protection is Data Minimization i.e. collect what you need! In our view the inclusion of NINs in court and arbitration processes is unnecessary. We fail to see how the non – provision of such information affects the substance of a case or the administration of justice. Furthermore, we believe NINs as Sensitive Personal Data should be given a higher level of protection and should not be easily accessible by mere application for Certified True Copies of court processes. The effect of this is that a lawyer's NIN becomes information accessible to the world and has the possibility of jeopardizing a lawyer's right to privacy. Perhaps the following provisions of Article 87 of the EU GDPR ought to be included in our jurisprudence:

> *"Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application.* ***In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation (emphasis ours)."***

While we ponder on the usefulness or otherwise of the inclusion of court and arbitration processes as part of the transactions for which inclusion of NIN is mandatory, bearing in mind that a lawyer typically includes his or her seal as issued by the Nigerian Bar Association and other Personal Data such as telephone numbers and address for service, the NIN Regulations has come to stay and is firmly backed-up by the NIMC Act; therefore, Data Controllers such as courts, arbitration panels/institutions are to be mindful of the requirement of the NDPR with regards to data security and audit of data collection, processing, storage processes and NDPR compliance in general.

For further information on the foregoing (none of which should be taken as legal advice), please contact:

Oyeyemi Oke (oyeyemi.oke@ao2law.com) or
Bidemi Olumide (bidemi.olumide@ao2law.com) or
Kitan Kola-Adefemi (kitan.kola-adefemi@ao2law.com)