A COMMENTARY ON THE NIGERIAN DATA PROTECTION BILL 2023

On Tuesday 4 April 2023, the President of the Federal Republic of Nigeria delivered the Nigerian Data Protection Bill 2023 ("the Bill") to the Senate and House of Representatives chambers of the National Assembly for their consideration. At the Senate, the Bill is numbered SB. 1114 while it is numbered HB. 2203 at the House of Representatives. The Bill has had a chequered history from when it was first presented for public comments as a draft document by the Honourable Minister of Communications and Digital Economy ("the Minister") in 2020 and subsequently in 2022. Now, the document is formally before the National Assembly and can be officially referred to as a Bill.

The Bill in its explanatory memorandum seeks to provide a legal framework for the protection of personal information and establish the Nigerian Data Protection Commission ("the Commission") for the regulation of the processing of personal information, and for related matters. On Wednesday 5 April 2023, the Bill was read for the first time at both the Senate and House of Representatives. On Thursday 6 April 2023, the Bill was read for a second time at the House and committed to the House Committee of the Whole. In this note, I highlight some of the pertinent provisions of the Bill and what they mean in practice for covered organisations. I also highlight the likely next steps in the legislative history of the Bill until presidential assent.

Scope of the Bill

Clause 2 of the Bill sets out the material scope of the Bill. According to this provision, the Bill shall apply where the:

a) data controller or data processor is domiciled in, resident in, or operates in Nigeria;
b) data processing operation occurs within Nigeria; or
c) data controller and processor not being domiciled, resident or operating in Nigeria, process the personal data of a data subject in Nigeria.

The Bill defines a data controller as 'an individual, private entity, public commission or agency or anybody who or which, alone or jointly with others, determines the purposes and means of the processing of personal data' while a processor is defined as 'an individual, private entity, public authority or any other body, who or which processes personal data on behalf of or at the direction of a data controller or another data processor'.

Clause 3 exempts particular processing operations, some of which are the processing of personal data carried out by one or more persons solely for personal or household purposes. Other processing operation exempted are those carried out by a 'competent authority' for the purposes of prevention, investigation, detection, prosecution, or adjudication of a criminal offence or the execution of a criminal penalty, or as is necessary for national security. The definition of competent authority in the Bill is so broad that it spans all the arms of government at all levels of government in Nigeria.

Definition of personal data and sensitive personal data

The Bill defines personal data to mean 'any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual'. From this definition, it is not clear

whether the use of individual refers to both living and deceased individuals. In addition, the explanatory memorandum refers to 'personal information' while the Bill makes copious references to 'personal data' which it defines. Therefore, it is unclear whether personal information and personal data mean the same thing.

Sensitive personal data is defined to mean personal data relating to an individual's genetic and biometric data, race or ethnic origin, religious or similar beliefs, health status, sex life, political opinions or affiliations, trade union memberships or other information as may be prescribed by the Commission.

Principles of data processing

Clause 19 of the Bill sets out the principles governing the processing of personal data and these are the main responsibilities of covered organisations. In other words, these key principles serve as the conditions that must cumulatively be complied with every time personal data is processed. Under the Bill, these principles are;

a) lawfulness, fairness and transparency which essentially means that personal data must be processed only if a legal ground exists, and must be in a fair and transparent manner with respect to the individual whose personal data is processed;
b) collected for specific, explicit and legitimate purposes, and not be further processed in a way incompatible with these purposes. Data processing is specific if the purpose is sufficiently defined, it is explicit if sufficiently unambiguous and clearly expressed and legitimate where it complies with legal provisions;
c) adequate, relevant, and limited to the minimum necessary for the purpose pursued by the processing operation. Essentially this means that the data collected must be necessary and proportional to accomplish the purpose of the processing;
d) retained for no longer than necessary;
e) accurate, complete, not misleading and where necessary kept up to date having regard to the purpose of the processing; and
f) processed in a manner that ensures appropriate security of the personal data.

Lawful basis of personal data processing

Clause 20 sets out the conditions that must be satisfied for the processing of personal data to be lawful and thus not prohibited. Unlike the data protection principles which cumulatively apply, it is sufficient if at least one of the lawful basis can be identified to legitimise a data processing operation. These conditions are; consent of the data subject; the processing is necessary for the performance of a contract, the processing is necessary for compliance with a legal obligation; the processing is necessary to protect the vital interest of the data subject or other person; the processing is necessary for performance of a task carried out in public interest or in the exercise of official authority vested in the data controller or processor; the processing is necessary for the purpose of legitimate interest pursued by the data controller or processor, or by a third party to whom the data is disclosed.

Data protection impact assessment

Clause 23 (4) of the Bill states that a data protection impact assessment (DPIA) is a process designed to identify the risks and impacts of an envisaged data processing operation. A data controller is required by clause 23 (1) to conduct a DPIA prior to a processing operation, in every circumstance where the processing of personal data may likely result in a high risk to the

rights and freedoms of a data subject by virtue of its nature, scope, context and purposes. In this regard, I note that the trigger for a DPIA under the Bill differs from that under the Nigerian Data Protection Regulations 2019 (NDPR) issued by the National Information Technology Development Agency (NITDA) where it is required that a DPIA must be conducted in data processing operations involving the 'intense' use of personal data.

Appointment of data protection officers

Clause 27 requires data controllers to designate a data protection officer (DPO) who shall be a person of expert knowledge of data protection law and practices having the ability to carry out the tasks prescribed by the Bill. The DPO may be an employee of the data controller or engaged by a service contract.

Rights of the data subjects

The Bill enshrines in clauses 29, 31-33 the various rights of data subjects to be observed and respected by covered organisations and these rights are; right to obtain certain information from the data controller without constraint or unreasonable delay; to withdraw consent; to object to certain type of processing operations; right not to be subject to a decision based on automated processing of personal data including profiling which produces legal or similar significant effects concerning the data subject; and right to data portability. In setting out the rights of the data subject, I note that the rights to correction, erasure and restriction of processing are not stand-alone rights but rather are listed under the type of information a data subject has the right to request from the data controller.

Cross-border transfers of personal data

Clause 36 (1) (a) of the Bill provides that personal data shall not be transferred from Nigeria to another country unless the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanisms that affords an adequate level of protection with respect to the personal data. In this regard I note the following; first, the concept of transfer is not defined so it is not clear whether it also includes accessing personal data physically located in Nigeria by a recipient that is physically outside of Nigeria. Second, the scope of this provision is restricted to only transfers to another country and does not include transfers made to another territory or an international organisation. Thirdly, 'adequate level of protection' as used in other data protection frameworks applies to only laws, and not to binding corporate rules, contractual clauses, and codes of conduct. Lastly, it is unclear, the exact breadth of contractual clauses contemplated as being subject to a contractual clause is not the same thing as being a party to the contract containing the contractual clauses.

Clause 38 also provides other grounds that can legitimise the transfer of personal data outside of Nigeria and they are; consent of the data subject; 'transfer is necessary for the performance of a contract to which a data subject is a party to…'; transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; transfer is for the sole benefit of a data subject; transfer is necessary or important for reasons of public interest; transfer is necessary for the establishment, exercise or defence of legal claims; or transfer is necessary to protect the vital interests of the data subject or of another person.

Registration of data controllers and processors

Clause 39 provides that data controllers and processors of 'major importance' are required to

register with the Commission within six months after the commencement of the Bill (when enacted) or upon becoming a data controller or processor of major importance. Clause 40 provides that the Commission may prescribe registration fees or levies to be paid by data controllers and processors of major importance.

Enforcement Authority

Clause 4 (1) establishes the Commission. Clause 6 (a) empowers the Commission to oversee the implementation of the provisions of the Bill. Accordingly, clause 41 authorises the Commission to investigate any complaint arising from the provision of the Bill. In conducting an investigation, the Commission has a lot of tools at its disposal such as powers to order a person to attend for oral examination, produce documents or furnish statement in writing made under oath. Pursuant to clauses 42 and 43 respectively, the Commission is authorised to issue a compliance order against a data controller or organisation and an enforcement order against a data controller or processor. While a compliance order may be a warning that certain acts constitute a violation, an enforcement order imposes a sanction.

Penalty provisions

Under clause 43 (3), depending on whether the data controller or processor is of major importance, the Commission may issue a penalty fee as part of its enforcement order which could range from N2,000,000 to two percent of the annual gross revenue in the preceding financial year. Clause 44 provides that a data controller or processor who fails to comply with an order of the Commission is guilty of an offence and liable upon conviction to a fine, imprisonment for a term not exceeding a year or both fine and imprisonment.

Status of the NDPR

It is pertinent to state that the Bill does not seek to repeal the NDPR. This is clearly expressed in Clause 59 (2) (f) which among other things provides that all regulations issued by NITDA or the Nigerian Data Protection Bureau (NDPB) shall continue in force as if they were issued by the Commission until repealed. This means that unless repealed or withdrawn the NDPR will concurrently apply with the Bill when it is enacted into law. However, where there exists a conflict in the NDPR and the Bill (when enacted), the provisions of the Bill as an Act will prevail over the NDPR because according to established case law in Nigeria, it is a trite principle of law that a subsidiary (or subordinate) legislation (such as the NDPR) cannot contradict or over- ride an Act enacted by the legislature.

Next steps

It appears that the Bill will be given speedy consideration at the National Assembly. However, as I have written elsewhere, there are currently three Bills on data protection before the National Assembly which according to legislative rules and practice must be consolidated with the Bill or withdrawn by their sponsors. In addition, I expect a public hearing on the Bill would be held in the next couple of weeks by a joint committee comprised of members of each chamber of the National Assembly. At the public hearing, stakeholders such as the Minister, NITDA, NDPB, civil society, human rights organisations, data protection experts and lawyers are likely to attend to make submissions supporting or opposing the Bill. On this basis, I note that some parts of the Bill remain unclear and contains some inconsistencies which may be highlighted for amendment during the public hearing.

A COMMENTARY ON THE NIGERIAN DATA PROTECTION BILL 2023

After this public hearing, the Bill would be passed by each chamber and delivered to the President for his assent, which I expect would happen ahead of the inauguration of the incoming administration on 29 May 2023.

Conclusion

Stakeholders have looked forward to the enactment of a robust data protection legislation in Nigeria. While the NDPR is in force and currently regulates the processing of personal data in Nigeria, stakeholders are still divided on whether NITDA does have the legal authority to issue it although this question has not been tested in court as of the time of this writing. In addition, the NDPR does have several limitations, one of which is the absence of legitimate interest as a legal base for the processing of personal data.

In any case, if the Bill eventually becomes law, one of the policy objectives of pillar #1 of the National Digital Economy Policy and Strategy (2020 – 2030), which is to enact a data protection law for Nigeria would have been met, courtesy of the sustained efforts of the Minister.

Contact person for this article

Chukwuyere Izuogu LL.M (Hannover), CIPP/E
chukwuyere@sskohn.com