Nigeria Data Protection Act: What Individuals, Businesses And Organizations Should Know

JUNE 22, 2023

On June 12, 2023, President Bola Ahmed Tinubu signed the *Nigeria Data Protection Act, 2023* into law (**"Data Protection Act"** or **"the Act"**). This marked a significant watershed in the country's journey towards developing a primary legislative framework for the protection of personal information of natural persons residing or doing business in Nigeria.

Prior to the enactment of the Act, there have been attempts at ensuring the protection of personal data in Nigeria by the relevant government agencies through subsidiary legislation, such as the *Nigeria Data Protection Regulation 2019* (**"Data Protection Regulation"**), issued by the National Information Technology Development Agency (**"NITDA"**). While the Data Protection Regulation may have filled the gap for some time in Nigeria, being a secondary source of law with a weaker legal and judicial weight, it does not provide enough comfort to foreign investors and partners who are becoming increasingly averse to data porous operating environments and markets.

In today's digital world, where large volumes of data are being generated, stored, and processed online,

privacy and data protection have become a top priority for many countries, businesses, and individuals alike. The imperative of safeguarding citizens' privacy and data rights led to a joint effort between the Nigeria Data Protection Bureau (**"NDPB"** or the **"Bureau"**) and the International Development Association (a member of the World Bank Group), through the *Nigeria Digital Identification for Development Project* (**"NID4D"**), which eventually culminated in sponsoring the Bill that gave birth to the Data Protection Act.

The Act provides, among others, for governing framework for processing personal data; rights of a

data subject; data security; cross-border transfer of personal data; requirements for data controllers and data processors of major importance; compliance, infringements, penalties, and dispute resolution; and the establishment of the Nigeria Data Protection Commission (the **"Commission"**), as an independent body to superintend and regulate data protection matters, and enforce compliance with the provisions of the Act.

This article highlights the objectives of the Data Protection Act and provides a synopsis of the key provisions that may be of interest to individual data subjects, as well as corporate entities and organizations processing personal data in the course of their operations.

* What purpose is the Act expected to serve?

The Data Protection Act is designed to:

- protect the rights of data subjects by ensuring that personal data is processed in a fair, lawful and accountable manner;
- promote data processing practices in Nigeria that guarantee the security of personal data and ensure the privacy of data subjects;
- provide the legal framework for regulating and safeguarding personal data, and the means of recourse and remedies where the rights of data subjects have been breached;
- ensure that data controllers and data processors fulfil their obligations to data subjects;
- safeguard data subjects' fundamental and constitutional rights, freedom and interests, and establish an impartial, independent and effective regulatory body to supervise data controllers and data processors and superintend over data protection and privacy issues; and
- strengthen the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through beneficial and trusted use of personal data.

The Act defines a *"data processor"* as an individual, private entity, public authority, or any other body, who processes personal data on behalf of, or at the direction of, a data controller or another data processor. It also defines a *"data controller"* as an individual, private entity, public commission, agency, or any other body who (alone or jointly with others) determines the purposes and means of processing of personal data.

* Scope & priority of the Act

The scope of application of the Act extends to automated and non-automated data processing, and only in instances where (a) the data controller or data processor is domiciled or resident or operating in Nigeria; (b) the processing of personal data occurs within Nigeria; or (c) where the data controller or data processor is NOT domiciled or resident or operating in Nigeria, but is processing personal data of a data subject that is in Nigeria.

Essentially, the Act applies to companies or entities incorporated and established under Nigerian law to carry on business in Nigeria, and those which, though not incorporated under Nigerian law or established in the country, have operations that extensively utilize the personal data of Nigerian residents and citizens in their day-to-day business.

It should be noted that the Act does not cover the processing of personal data carried out solely for personal or household purposes. However, this exemption applies only where such processing does not constitute a violation of a data subject's fundamental right to privacy.

The Act takes priority over any other law or enactment relating directly or indirectly to the processing of personal data of data subjects in Nigeria, and the provisions of the Act shall prevail over any inconsistent provisions in any other law or enactment on personal data processing.

* Governing framework for processing personal data

Personal data & sensitive personal data

The Act prohibits unlawful processing of personal information, which consists of personal data and sensitive personal data of natural persons.

For the purposes of the Act, *"personal data"* means any information relating directly or indirectly to an identified or identifiable individual, 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.

The Act also defines *"sensitive personal data"* as personal data relating to an individual's — (a) genetic and biometric data, for the purpose of uniquely identifying a natural person; (b) race or ethnic origin; (c) religious or similar beliefs, such as those reflecting conscience or philosophy; (d) health status; (e) sex life; (f) political opinions or affiliations; (g) trade union memberships; or (h) other information which may be prescribed by the Commission as sensitive personal data.

Basic principles

The Act sets the minimum principles to guide the processing of personal data. For instance, a data controller or data processor owes a duty of care, in respect of data processing, and is required to demonstrate a high level of accountability. Therefore, a data controller or data processor is required to use appropriate technical and organizational measures to ensure confidentiality, integrity, and availability of personal data.

In addition to the requirement to process personal data in a fair, lawful and transparent manner, a data controller or data processor is also required to collect personal data only for specified, explicit, and legitimate purposes, and not to engage in any further processing of collected data in a way that is incompatible with the original purposes. The collected data must also be accurate, complete, kept to date, adequate, relevant, not misleading, and limited to the minimum necessary for the purposes for which it was collected or further processed.

Furthermore, collected data is not to be retained for longer than is necessary to achieve the lawful bases for which it was collected and is to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach.

However, a data controller or data processor will be free from obligations under the Act regarding processing of personal data, where it is shown that the processing is 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, in accordance with any applicable law;
- prevention or control of a national public health emergency; and
- national security, as may be necessary.

Furthermore, a data controller or data processor will not be liable for noncompliance with the provisions of the Act, where it can be proven that processing of personal data is:

- in respect of publication (in the public interest) for journalism, educational, artistic and literary purposes, to the extent that such purposes are incompatible with the obligations and rights; or
- necessary for the establishment, exercise, or defense of legal claims, whether in court proceedings, or in an administrative or out-of-court procedure.

The foregoing exemptions will only be available to a data controller or data processor subject to the rights and freedoms guaranteed under the Constitution and the limitations thereof, and without prejudice to the prescribed principles and lawful basis for personal data processing, statutory role of Data Protection Officers, and obligations of data processors and data controllers in the event of a data breach under the Act.

Consent as lawful basis

The primary lawful basis for processing personal data is the consent of the data subject, freely and intentionally given, and not withdrawn, for the specific purpose or purposes for which the personal data is to be processed. The burden of proof for establishing a data subject's consent lies on the data controller, and silence or inactivity of the data subject shall not constitute consent. However, data processing will be lawful without consent, where the processing is

necessary for certain reasons including the following:

- for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract (except where this will override the fundamental rights, freedoms and the interests of the data subject or the processing is incompatible with other lawful basis of processing or the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged);
- for compliance with a legal obligation to which the data controller or data processor is subject;
- to protect the vital interest of the data subject or another person, where the data subject is physically or legally incapable of giving consent;
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor;
- for the purposes of the legitimate interests pursued by the data controller or data processor, or by a third party to whom the data is disclosed;
- for the establishment, exercise, or defense of a legal claim, obtaining legal advice, or conduct of a legal proceeding; and
- for reasons of substantial public interest, on the basis of a law, which shall be proportionate to the aim pursued, and provides for suitable and specific measures to safeguard the fundamental rights, freedoms and interests of the data subject.

Consent of a child or person lacking legal capacity

Where a data subject is a child or a person lacking the legal capacity to give consent, a data controller is required to obtain the consent of the parent or legal guardian (as applicable). In doing this, appropriate mechanisms are required to be applied to verify age and consent, taking into consideration available technology. The presentation of any government approved identification documents suffices as an appropriate mechanism.

A "child" under the Data Protection Act has the same meaning as ascribed in the Child's Right Act. Thus, anyone under the age of 18 shall be taken to be a child for data protection purposes. It is noteworthy that the definition has effectively invalidated the provision in the NITDA's *NDPR: Implementation Framework* which qualifies anyone under the age of 13 as a child. However, the Act empowers the Commission to make appropriate regulations where the circumstance relates to the processing of personal data of a child of 13 years and above, requiring the provision of information and services by electronic means at the specific request of the child.

However, the consent of the parent or legal guidance will not be required where the data processing is necessary to protect the vital interests of the child or person lacking the legal capacity to give consent; or where the processing is carried out for purposes of education, medical or social care, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or where the processing is necessary for proceedings before a court relating to the individual.

* Rights of a data subject

A data subject under the Act has the right to obtain confirmation from a data controller or data processor, as to whether the data to be processed will be stored, or whether the data is personal data relating to the data subject. Where any of the foregoing is confirmed to be the case, the data subject has the right to be

informed of the following, without constraint or unreasonable delay:

- purposes of the processing;
- categories of personal data concerned;
- recipients or categories of recipient to whom the personal data have been or will be disclosed (particularly recipients in third countries or international organizations),
- period for which the personal data will be stored, or the criteria used to determine that period;
- existence of the right to request for rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject or to object to such processing;
- right to lodge a complaint with the Nigeria Data Protection Commission;
- available information as to the source of personal data, where it is not collected from the data subject; and
- existence of automated decision-making including profiling, as well as the significance and envisaged consequences for the data subject.

In addition to the above, a data subject has the right to withdraw previously given consent to the processing of his personal data at any time. Where consent is withdrawn, a data controller is under obligation to discontinue the processing of personal data, unless the data controller demonstrates a public interest or other legitimate grounds, which overrides the fundamental rights and freedom, and the interests of the data subject.

In like manner, but subject to regulations made by the Commission, a data subject has a right of personal

data portability. This entitles the data subject to receive (without undue delay) personal data relating to him/her from a data controller, in a structured, commonly used, and machine-readable format. Under the right, the data subject may also transmit the personal data received in this format to another data controller without hindrance and may have it transmitted directly from one data controller to another, where technically possible.

* Data security

Adequate data protection

The Data Protection Act places a legal obligation on a data controller or data processor to ensure the security, integrity and confidentiality of personal data in its possession or under its control. To this effect, a data controller or data processor is mandated to implement appropriate technical and organizational measures to ensure this, including protection of the personal data against accidental or unlawful destruction, loss, misuse, alteration, and unauthorized disclosure or access.

In doing this, the Act requires data controllers or data processors to take certain things into account including the following:

- amount and sensitivity of the personal data;
- nature, degree and likelihood of harm to a data subject that could result from the loss, disclosure, or other misuse of the personal data;
- extent of the processing;
- period of data retention; and
- availability and cost of any technologies, tools, or other measures to be implemented relative to the size of the concerned data controller or data processor.

Some of the measures that may be implemented by a data controller or data processor, to ensure adequate protection of the information of a data subject include (i) pseudonymization or other methods of de-identification of personal data (ii) encryption of personal data (iii) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services (iv) processes to restore availability of and access to personal data in a timely manner, in the event of a physical or technical incident (v) periodic assessments of risks to processing systems and services, including where the processing involves the transmission of data over an electronic communications network (vi) regular testing, assessing, and evaluation of the effectiveness of the measures implemented against current and evolving risks identified, among others.

Personal data breach

In the event of a breach of personal data, the Act requires a data processor to promptly inform the data controller, describing the nature of the breach and, where possible, give information about the categories and approximate number of data subjects affected. The data processor shall also promptly respond to all information requests from the data controller for the purpose of compliance with the provisions of the law regarding personal data breach. In the same vein, the data controller on its part is required to inform the Commission of the breach, within 72 hours of becoming aware of a breach that is likely to result in a risk to the rights and freedoms of data subjects, and where feasible provide a detailed description of the breach.

* Cross-border transfer of personal data

The Act prohibits the transfer of personal data from Nigeria to another country by a data controller or data processor, unless the recipient of the personal data is subject to a law, binding corporate rules, contractual

clauses, code of conduct, or certification mechanism that affords an adequate level of protection with respect to the personal data, or where the transfer aligns with the acceptable basis for processing of data under the Act.

The Act permits the transfer of personal data to another country only if there is adequate level of protection in that country, and the data controller or data processor is required to record the basis of such transfer and the adequacy of protection. The Act empowers the Commission to make regulations requiring data controllers and data processors to notify it of the measures in place to guarantee protection of personal data in cross-border transfer, and to explain the adequacy of such measures. By the same token, the Commission may make regulations designating categories of personal data that are subject to additional specified restrictions on transfer to another country, based on the nature of such personal data and risks to data subjects.

Adequate level of protection under the Act refers to the capability or sufficiency of the data protection mechanisms in place in the recipient country; and this is to be measured based on guidelines to be issued by the Commission, as well as by using the following criteria:

- availability of enforceable data subject rights and the ability of a data subject to enforce such rights through administrative or judicial redress, and the rule of law;
- existence of any appropriate instrument between the Nigeria Data Protection Act and a competent authority in the recipient jurisdiction that ensures adequate data protection;
- access of a public authority to personal data;
- existence of an effective data protection law;
- existence and functioning of an independent, competent data protection, or similar supervisory authority with adequate enforcement powers; and
- adequacy of international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organizations.

The Act provides for conditions under which personal data may be transferred abroad in the absence of adequate protection. Such conditions include cases where consent of the data subject has been provided to the transfer, after having been informed of the possible risks of such a transfer; or where the transfer is necessary for important reasons of public interest; and where the transfer is necessary for the establishment, exercise, or defense of a legal claim, among others.

* Requirements for data controllers and data processors of major importance

The Act mandates data controllers and data processors of major importance to register with the Commission, within six (6) months of the commencement of the Act or upon attaining the status. Under the Act, a "data controller or data processor of major importance" refers to a:

> *"data controller or data processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Nigeria Data Protection Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate."*

Registration requirements include the provision of the following information to the Commission by a qualified data controller or data processor:

- name and address of the data controller or data processor, and name and address of the data protection officer (**"DPO"**) of the data controller or data processor;
- a description of personal data and the categories and number of data subjects to which the personal data relate;
- purposes for which personal data is processed;
- categories of recipients to whom the data controller or data processor intends or is likely to disclose personal data;
- name and address, or name and address of any representative of any data processor operating directly or indirectly on its behalf;
- country to which the data controller or data processor intends, directly or indirectly to transfer the personal data;
- a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data; and
- any other information required by the Commission.

From the wording of the Act, it appears that the designation and registration of data controllers and data processors of major importance may not commence until the Commission issues a regulation stipulating the eligibility criteria for being so designated, as well as a guideline prescribing the appropriate registration fees or levies for qualified data controllers and data processors. However, the Act empowers the Commission to exempt a class of data controllers or data processors of major importance from the stated registration requirements, where it considers such requirements to be unnecessary or disproportionate.

* Compliance, infringements, penalties, and dispute resolution

Data controllers and data processors are under legal obligation to comply with the provisions of the Act, as well as the provisions of regulations, guidelines and any other subsidiary legislation made pursuant to the Act. Infringement of the provisions of the Act or any relevant subsidiary legislation attracts appropriate orders by the Commission, where it is satisfied that a data controller or data processor has violated or is likely to violate any requirement under the Act or the subsidiary legislation.

In appropriate circumstances, the Commission may make compliance orders, warning the affected data controller or data processor about a specific violation of the Act, or requiring immediate compliance with the specific provisions of the law breached or likely to be breached, or directing a data controller or data processor to cease and desist or refrain from doing an act which is in violation of the Act or a subsidiary legislation made under the Act.

Similarly, the Commission, upon completion of investigation of any complaint lodged against a data controller or data processor, may make enforcement orders where it is satisfied that the data controller or data processor has violated the provisions of the Act or any relevant subsidiary legislation. The enforcement order may impose a sanction on the data controller or data processor or direct it to do anything in furtherance of the objectives of the Act or for the sake of justice, or to pay penalty or remedial fee. A person who is not satisfied with an order of the Commission, may apply to a court of competent jurisdiction for judicial review, within 30 days after the order was made.

A data controller or data processor who fails to comply with orders made by the Commission commits an offence under the Act. In the case of a data controller or data processor of major importance, it shall be liable on conviction to a fine of up to ten million naira (₦10m) or 2% of its annual gross revenue in the preceding financial year, whichever is greater. A data controller or data processor not of major importance shall, upon conviction, be liable to a fine of up to two million naira (₦2m) or 2% of its annual gross revenue in the preceding financial year, whichever is greater. A convicted data controller or data processor may also be liable to both fine and imprisonment for a term not more than one year. Similarly, a court may make any appropriate order including an order of forfeiture against a convicted data controller, data processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act.

A Judge may issue a warrant for the purpose of obtaining evidence in relation to an investigation, upon an *ex-parte* application filed by the Commission, where the court is satisfied that a person has engaged, is engaging, or is likely to engage in a conduct that contravenes the Act. The warrant sought should be for the purpose of preventing a crime or preventing interference with investigative process, or for the purpose of investigating data security breaches and data privacy breaches or obtaining electronic evidence.

Regardless of any criminal sanctions under the Act, a data subject who suffers injury, loss, or harm due to a violation of the Act by a data controller or data processor, may recover damages from such data controller or data processor in civil proceedings.

Where an offence has been committed under the Act by a company or corporate entity, the entity as well as its principal officers shall be deemed culpable, unless the principal officers prove that (i) the offence was committed without their consent or connivance; and (ii) they exercised diligence to prevent the commission of the offence. A data controller and data processor shall be vicariously liable for the acts or omissions of its agent or employees, in so far as the acts or omissions relate to its business.

* Transition to the new regime

The Act makes saving provisions preserving existing institutions and administrative actions in relation to data protection. Thus, a reference to the NDPB before the commencement of the Act or a document issued in the name of the Bureau, shall be read as a reference to the Commission. In like manner, all persons engaged by the Commission shall have the same rights, powers and remedies as existed in the Bureau while all officers and employees of the Bureau shall continue in office and be deemed to have been appointed under the Act. Also, all existing agreements and contracts, records and equipment of the Bureau shall become that of the Commission.

By the same token, all orders, rules, regulations, decisions, directions, licenses, authorizations, certificates, consents, approvals, declarations, permits, registrations, rates or other documents that are in effect before the coming into effect of the Act and that are made or issued by the NITDA or the NDPB shall continue in effect as if they were made or issued by the Commission until they expire or are repealed, replaced, reassembled or altered.

Remarks

The Nigeria Data Protection Act is a welcome development, coming at a time Nigeria is taking great strides towards the full realization of a digital economy. Notably, the digital economy is data-based and data-driven. Any nation that aims to onboard a digital economy must not only invest in digital technologies but also have in place a reliable national database, that is supported by a strong and effective data protection statute. It is expected that the Act will boost the confidence of all Nigerian citizens and residents to fully support the country's digital economy ambition. The full implementation of the Act

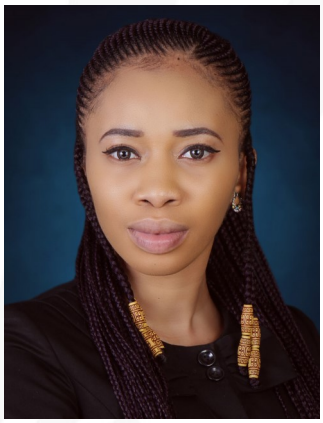
will improve the business environment in Nigeria and increase investor confidence, as companies will have a clear set of guidelines to follow when collecting and processing personal data. The Act will also enhance Nigeria's reputation as a safe and secure place to do business, attracting more foreign investment and boosting economic growth.

Banwo & Ighodalo played a pivotal role in the emergence of the Data Protection Act, through the provision of advisory, consultative and advocacy services to the NID4D, with the support of the World Bank. Specifically, this was through facilitating consultative and advisory sessions with members of the National Assembly towards the passage of the Executive Bill as well as engagements with the Executive towards its assent into law.

Contact Persons:

Olumide Osundolire
Partner
E: oosundolire@banwo-ighodalo.com

Toyin Bashir
Partner
E: tbashir@banwo-ighodalo.com



Thelma Okorie
Associate
E: tabu@banwo-ighodalo.com

Oluwatoba Oguntuase
(Senior Practice Support Lawyer)
E: ooguntuase@banwo-ighodalo.com