THE DATA PROTECTION ACT 2023: SAFEGUARDING THE PRIVACY RIGHTS OF DATA SUBJECTS IN NIGERIA

GBENGA BIOBAKU & CO
BARRISTERS & SOLICITORS

Introduction

On June 12, 2023, President Bola Ahmed Tinubu signed the Nigeria Data Protection Act, 2023 (DPA) into law. Before the DPA was passed, the primary protective legislation for the personal data of Nigerians was the Nigeria Data Protection Regulation 2019 which was issued by the National Information Technology Development Agency ("NITDA"). NITDA set out the regulations with regard to the processing of information relating to identifiable individuals' personal data, including the obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, use and disclosure.

In today's digital age, the protection of personal information has become paramount. With the enactment of the Data Protection Act 2023 (DPA) in Nigeria, the safeguarding of fundamental rights and freedoms of individuals has gained significant attention. Against this backdrop, we have extensively reviewed the provisions of the Act especially relating to the rights of data subjects' vis-a-vis the salient obligations imposed on data controllers/processors as well as the legal consequences where any of these is violated by the data controllers/processors.

Objectives Of The DPA

In an era driven by digital technologies and an ever-expanding data landscape, the protection of personal information has become paramount. Recognizing the significance of safeguarding the fundamental rights, freedoms, and interests of individuals, **Section 37** of Nigerian Constitution laid the groundwork for a legislation dedicated to the regulation of processing personal data by guaranteeing the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. It is important to note that the DPA describes personal data as nay information relating to an individual who can be identified directly or indirectly by reference to an identifier such as a name, identification number, biometric data, location data including an online identifier relating to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.

Over time, there have been series of reports on how the information of data subjects are being used indiscriminately and violated by data controllers and data processors alike without the clear consent of the data subjects and without legal authorization. According to a report by a cybersecurity company, Surfshark, Nigeria recorded 82,000 incidents of data breach between January to March 2023. With this development, Nigeria ranks 32nd on a list of countries with the most data breaches in the first quarter of 2023. The DPA was therefore enacted in response to the increasing reports of data breaches and privacy violations affecting Nigerians. By introducing comprehensive regulations, the DPA seeks to curb the exchange of sensitive personal data without consent, establish legal safeguards, and enforce accountability.

Objectives Of The DPA *Contd.*

Consequently, the Data Protection Act 2023 (the "DPA or the Act") has been enacted to checkmate the activities of data controllers or processors alike who exchange sensitive information of data subjects with one another without their consents, provide procedure and manner through the consent of data subjects can be sought and procured. The DPA states that data controllers are individuals, private entities, public commissions, agencies or any other body who alone or jointly with others determines the purposes and means of processing of personal data whilst data processors are individuals, private entities or any other body who processes personal data on behalf of or at the direction of a data controller. The DPA not only aims to ensure the security and privacy of data subjects but also establishes a framework for fair and accountable practices. Moreover, the DPA seeks to enforce the responsibilities of data controllers and processors while providing effective means of recourse and remedies in the event of a breach. The Act also makes provisions for legal sanctions where data controllers or processors violate the rights of data subjects without lawful justifications or reasons.

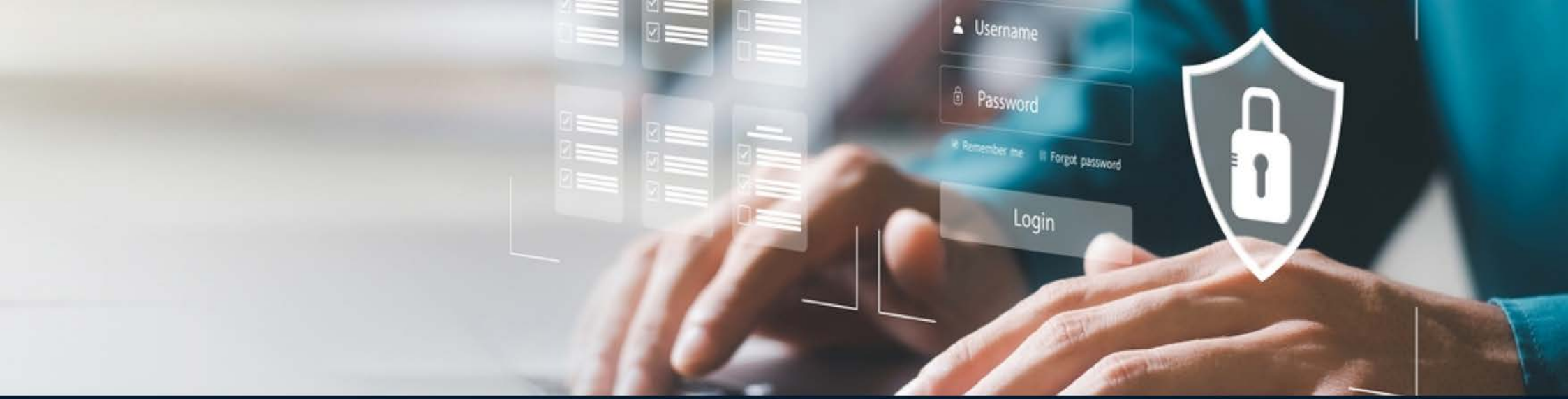
Applicability Of The DPA

The application of the DPA cut across all data processing activities be it automated or non-automated. It also applies to all data controllers and data processors domiciled and operating in Nigeria including the ones domiciled abroad but is processing the personal data of a data subject in Nigeria.

However, the provisions of the Act does not apply where the processing of personal data is carried out by one or more persons solely for personal or household purposes provided that it does not violate the right of privacy of a data subject. Additionally, the DPA does not apply to a data processor or controller where the data processing is carried out by a competent authority in a bid to prevent, investigate, prosecute a criminal offence or where such processing is carried out for the purpose of executing a criminal penalty in accordance with the law. Also, the application of the DPA can be put in abeyance for national security reasons, national health emergency and public interest etc.

Establishment Of The Data Protection Commission And Its Powers

The new law establishes the Nigeria Data Protection Commission (the "Commission") and replaces the NDPB established by former President Buhari in February 2022. The Act states that any references to the former Bureau and documents issued in its name should now be understood as references to the Commission. Furthermore, all individuals employed by the Commission will possess the same rights, powers, and remedies as they did in the Bureau. The DPA safeguards existing agreements, records, equipment, and properties, which will now be transferred to the Commission. Ongoing legal proceedings and documents issued by the National Information Technology Development Agency or the Bureau will continue to be in effect until expiration or any necessary amendments.



Principles And Lawful Basis Governing Processing Of Personal Data

The DPA 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, psychological, genetic, psychological, cultural, social or economic identity of that individual. By Section 4, the categories of data to which the Act applies include:

- Personal and biometric data revealing a data subject's identity, racial, or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or trade union membership
- Personal banking and accounting records;
- Personal data revealing a data subjects flight reservations or itinerary;
- Student's academic transcripts records;
- Telephone calls, call data records, messages, websites, and other information stored on any electronic device.
- Personal subscription

As mentioned above, the DPA does not apply to the processing of personal data carried out solely for personal or household purposes, provided it does not violate the fundamental right to privacy of the data subject. Certain obligations of the DPA do not apply to data controllers or processors in specific circumstances, including processing by competent authorities for criminal investigation, national public health emergencies, national security, public interest publications, and legal claims. The Commission can prescribe exemptions and issue guidance notices to ensure compliance and safeguard data subjects' rights.

Just like the Nigeria Data Protection Regulation, the DPA has imposed certain basic principles and rules on data controllers/data processors which must be observed when processing personal data of data subjects. Data processors and controllers who are responsible for using personal data have to follow strict rules called 'data protection principles". They must make sure the information is included in a privacy policy that is clear, concise, transparent, intelligible, and easily accessible. Additionally, if the processing of personal data poses a high risk to the rights and freedoms of a data subject, a data privacy impact assessment must be conducted, involving a systematic description of the processing, including an assessment of its necessity and risks, and measures to address those risks.

Data controllers and processors have a crucial responsibility to handle personal data in a manner that is fair, lawful, and transparent. They must collect data for specific purposes, ensuring it is relevant and limited to what is necessary. Therefore, they are to ensure that such personal data is not used for any other purpose other than the one it is assigned for or retain such data longer than necessary. The retention of data should also be for an appropriate time frame, and accuracy should be maintained. **Section 24 (1) of the Act.** Implementing stringent security measures is also essential to protect personal data against unauthorized access or unlawful processing, loss, destruction, damage or any form of data breach. Data processers are also mandated to use appropriate technical and organizational measures to ensure the confidentiality, integrity and availability of personal data. Additionally, data controllers and processors must demonstrate accountability and exercise a duty of care in adhering to the principles outlined in the DPA. Lawful processing can be based on consent, contractual obligations, legal requirements, or protection of vital interests.

Rights Of Data Subject Under DPA

Every data subject under the DPA has a right to confirm from the data controllers or data processors about the storage of his personal data. They also have the right to enquire about the purpose of the processing of their personal data, the categories of personal data concerned, the recipient or categories of recipients to whom such data will be disclosed and the period of time for which such data will be stored. Data subject also have the right to direct the data controller to either rectify or erase their personal data or restrict the processing of their personal data. **Sections 26, 27 & 34 of the Act.** Some of the key rights of a data subject under the DPA include:

(i.) Right to Access

(ii.) Right to Rectification and Erasure: Data subjects have the right to request the correction or deletion of inaccurate or misleading data held by data controllers

(iii) Right to receive a copy of their personal data in an electronic format, unless it imposes unreasonable costs

(iv.) Right to withdraw their consent

(v.) Right to Restriction of processing.

> Similarly, data subjects have the right to give clear consent before their personal data can be processed by data controllers/processors. Therefore, no data controller can process the personal data of a data subject without his consent. Such consent must be explicit and clear and not based on assumption. The burden of proof lies with the data controller to establish the consent of the data subject, ensuring it is freely given and not a condition for contract performance. Consent cannot be inferred from silence or inactivity **Section 30 of the Act.**

Notwithstanding the above, it is instructive to note that where the personal data involved is sensitive in nature, there are instances where the data controllers can process such data with or without the approval of the data subjects. For instance, where the processing is necessary to establish or defend a legal claim, obtain legal advice or conduct legal proceedings or where it is necessary for archiving purposes for public interest, and engaging in historical, statistical or scientific research or to carry out or provide medical care or community welfare or for safeguarding public health and to provide for suitable and specific measures to safeguard the fundamental rights, freedoms and the interests of the data subjects thereof. **Section 30 of the DPA.**

Furthermore, a data subject also has the right under **Section 36(1) of the Act,** to object to the processing of personal data relating to him/her by data controller/ processor; and where this happens, the data controller is mandated to discontinue same forthwith. However, such objection can be overridden where public interest is involved or where there are other legitimate grounds for processing such data. Therefore, the rights and freedoms of the data subject is of no moment in the such circumstances even if processing such data may violate the right of a data subjects.

On the issue of consent in data processing, where data of a child who lacks the legal capacity to give consent is involved, the data controller is obligated to obtain such consent from the parents or legal guardians of such child before processing the data of such child. **Section 31 of the Act.** The Commission is also empowered to make rules and regulations with regards to providing information and services via electronic means involving a child.

On the issue of consent in data processing, where data of a child who lacks the legal capacity to give consent is involved, the data controller is obligated to obtain such consent from the parents or legal guardians of such child before processing the data of such child. **Section 31 of the Act.** The Commission is also empowered to make rules and regulations with regards to providing information and services via electronic means involving a child.

> Furthermore, a data subject also has the right under Section 36(1) of the Act, to object to the processing of personal data relating to him/her by data controller/ processor; and where this happens, the data controller is mandated to discontinue same forthwith. However, such objection can be overridden where public interest is involved or where there are other legitimate grounds for processing such data. Therefore, the rights and freedoms of the data subject is of no moment in the such circumstances even if processing such data may violate the right of a data subjects.

Data Privacy Impact Assessment And The Obligations Of Data Controllers/Processors Under The Act

Every data controller/processor is required to carry out a prior data privacy assessment before processing personal data of data subjects. This is because of the level of high risk associated with data processing which affect the rights and freedoms of data subjects. Put differently, the data privacy impact assessment is designed to protect data subjects by identifying the risks and impacts of the envisaged processing of personal data which comprises of assessing the necessity and proportionality of processing in relation to the purposes for which personal data is being processed and taking measures to ensure the data security of data subjects.

Pursuant to Section 39 of the Act, data controllers/processors are obligated to implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data under their control. These measures should address risks such as loss, misuse, accidental or unlawful destruction, alteration, or unauthorized disclosure of data, taking into account factors like data sensitivity, potential harm to individuals and data retention period. Examples of such measures include encryption, data restoration procedures, risk assessments, regular testing, and updates to address emerging threats.

In cases where a data controller/processor engages the services of another data processor to carry out data processing on its behalf, it must ensure compliance with the principles and obligations imposed on data controllers as provided by the Act. Such data processor or controller must also make sure that the appropriate technical and organizational measures are put in place by the engaged processor to ensure the security, integrity and confidentiality of personal data as required under part VII are fully implemented. **Section 29 of the DPA.**

Data Privacy Impact Assessment And The Obligations Of Data Controllers/Processors Under The Act

Where a personal data breach has occurred with respect to personal data being stored or processed by a data processor, the data processor shall, on becoming aware of the breach, notify the data controller that engaged it, of such breach. The data controller is in turn required to inform the Commission of the breach, within Seventy -Two (72) hours of becoming aware of such breach, and where feasible, describe the nature of the breach including the categories and approximate numbers of data subjects and personal data records concerned. Such notifications and communications shall also describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Additionally, where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller shall immediately communicate the personal data breach to the data subject in plain and clear language, including advice about measures the data subject should take to mitigate effectively the possible adverse effects of the data breach. Section 40 of the DPA. In cases where such direct communication to the data subjects would involve disproportional effort or it is not feasible, the data controller is required to explore option of public communication in one or more widely used media source such that the data subject is likely to be informed. Also, the data controller is required to keep records of every data breach that occurs to data under its possession including facts relating to such breach, its effects and remedial actions taken in a manner that will enable the commission to verify compliance. Section 49(8) of the Act.

Trans Border Flow Of Personal Data

Generally, data controllers or processors cannot transfer personal data from Nigeria to another country unless certain conditions are met. Firstly, the recipient country must provide an adequate level of protection through its laws. The adequacy of protection is assessed by considering factors such as enforceable data subject rights, existence of a data protection law, and international commitments. The Commission can determine if a country, sector, or instrument provides adequate protection. Binding corporate rules, codes of conduct, or certification mechanisms may be approved by the Commission. In the absence of an adequacy determination, transfers may occur with data subject consent, contractual necessity, data subject's benefit, public interest, legal claims, or vital interests' protection. Data controllers or processors are obligated to record the basis for such transfer of personal data to a recipient abroad. **Section 41 & 42 of the DPA.**

Sanctions And Penalties

The DPA, pursuant to **Section 46,** empowers the Commission to investigate alleged violations by data subjects and issue appropriate compliance orders. Sanctions or orders may involve data controllers or processors compensating affected data subjects for losses or injuries resulting from personal data violations. The Commission may also order the data controller or processor to account for profits gained from such violations. Sanctions and orders by the Commission will depend on the nature, gravity, and duration of the violation

Conclusions

It is important to state that Data Protection Act does not expressly or impliedly repeal other existing laws or enactments directly or indirectly relating to the processing of personal data in Nigeria. Thus, the provisions of the Act are tailored to run alongside with such existing laws. However, where there is a conflict between the provisions of the DPA and such other laws and enactments, the provisions of the DPA shall prevail. **Section 63 of the Act.**

The transitional provisions under **Section 64 of the DPA** provides that any reference to the Nigeria Data Protection Bureau (the "Bureau") existing before the commencement of the DPA or a document issued in the name of the Bureau, shall be read as a reference to the Commission and all persons engaged by the Commission shall also have the same rights, powers and remedies as existed in the Bureau before the commencement of the Act. The implication of this is that the Act replaces the NDPB with the Commission established under the DPA but preserves the existing staff of the Bureau and existing agreements entered into by the Bureau before the commencement of the Act. Another implication of this is that data controllers or date processor organizations that process personal data of more than 1000 data subjects in a period of Six (6) months are still mandated to submit a soft copy of the summery of their Data Protection Audit Report, not later than the 15th of March of the following year, to the Commission. Also, Data Controllers that process the Personal Data of more than 2000 Data Subjects in a period of Twelve (12) months, are also obligated to submit a soft copy of the summery of their Data Protection Audit Report to the Commission on an annual basis, not later than the 15th of March of the following year.

The Data Protection audit which should cover the audit of the organizations privacy and data protection practices should state the following:

i. personally identifiable information the organization collects on employees

ii. of the organization and members of the public;

iii. any purpose for which the personally identifiable information is collected;

iv. any notice given to individuals regarding the collection and use of personal

v. information relating to that individual;

vi. any access given to individuals to review, amend, correct, supplement, or

vii. delete personal information relating to that individual

viii. whether or not consent is obtained from an individual before personally

ix. identifiable information is collected, used, transferred, or disclosed and

x. any method used to obtain consent;

xi. the policies and practices of the organization for the security of personally identifiable information;

The Nigeria Data Protection Act, 2023 marks a significant step in safeguarding the personal data of data subjects in Nigeria (be it a Citizen or Non-Citizen as long as they are in Nigerian) processed by data controllers or data processors domiciled, resident or operating in Nigeria. By replacing the previous regulations and introducing comprehensive provisions, the DPA aims to ensure the protection, security, and privacy of personal information of data subjects in Nigeria.

Disclaimer

Nothing in this article should be construed as legal advice from any of our lawyers or the firm. The article published is a general summary of developments and principles of interest and may not apply directly to any specific circumstances. Professional advice should therefore be sought before action based on any article is taken.

Contact Details

For more information, please contact:

Adetola Lawal
Partner
alawal@gbc-law.com

Adeola Fayose
Senior Associate
adeolafayose@gbc-law.com

GBENGA BIOBAKU & CO.
Barristers and Solicitors
11 Babafemi Osoba Crescent Off
Admiralty Road, Lekki Phase1, Lagos.
234 8023715888
+234 1 2717769
+234 1 2707320 (Fax)
info@gbc-law.com
http://www.gbc-law.com