ANDERSEN®

Overview of the Nigeria Data Protection Act, 2023

Ng.Andersen.com

June 2023

Content

ANDERSEN

Introduction

On 12 June 2023, the Nigeria Data Protection Act 2023 ("the Act") was signed into law by President Bola Ahmed Tinubu, GCFR. The Act provides a legal framework for the protection of personal information and establishes the Nigeria Data Protection Commission for the regulation of the processing of personal information. The objectives of the Act include:

- Safeguarding the fundamental rights and freedoms, and the interests of data subjects as guaranteed under the 1999 Constitution of the Federal Republic of Nigeria;
- Providing for the regulation of processing of personal data;
- Promoting data processing practices that safeguard the security of personal data and privacy of data subjects;
- Ensuring that personal data is processed in a fair, lawful and accountable manner;
- Protecting data subjects' rights and providing means of recourse and remedies, in the event of the breach of the data subjects' rights;
- Ensuring that data controllers and data processors fulfill their obligations to data subjects;
- Establishing an impartial, independent and effective regulatory Commission to superintend over data protection and privacy issues, andsupervise data controllers and data processors; and
- Strengthening the legal foundations of the national digital economy and guaranteeing the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data.

The Act sets out its scope, the lawful basis for processing personal data and prescribes penalties for non-compliance with its provisions. In the subsequent pages, we have highlighted provisions that may be of interest to data controllers and processors or third parties engaged by them and our comments.

ANDERSEN

Key comments on the Act

Notable Section	Highlights	Our Comments
Scope of Application Section 2	The Act shall apply to the processing of personal data, whether by automated means or not where the: • Data controller or data processor is domiciled in, resident in, or operating in Nigeria; • Processing of personal data occurs within Nigeria; or • The data controller or the data processor is not domiciled in, resident in, or operating in Nigeria but is processing personal data of a data subject in Nigeria.	The terms ***"domiciled", "resident"*** and ***"operating"*** were not defined in the Act but it is expected that the ordinary meanings of the words will be applied. This means that if a data controller or processor is operating in Nigeria then the provisions of the Act will apply to it. Furthermore, the provisions of the Act will apply where a data processor and controller is not resident in Nigeria but processes the data of data subjects in Nigeria. Based on the foregoing, the provisions of the Act could be interpreted to exclude Nigerian citizens who are abroad from its application.
Exemptions Section 3	This Section lists the exemptions to the application of the Act (fully or partially). This includes the processing of personal data solely for personal or household reasons. There are some partial exemptions for processing by competent authorities for the prevention or investigation of criminal acts, the prevention or management of a national public health emergency, and as required for national security. Furthermore, in the public interest, processing may be excused for journalism, education, artistic, and literary purposes, to the extent that such responsibilities and rights are incompatible with such objectives, or for the establishment, exercise, or defense of legal claims.	Data controllers or data processors may be subject to a number of exemptions if the processing activities undertaken by them can be captured under this section. It is crucial to note, however, that these exceptions do not grant an unlimited exemption from the Act's requirements. Section 3(4) authorises the Commission to issue a Guidance Notice to a data controller or processor containing legal safeguards and best practices in relation to any aspect of data processing exempted under this section where, in the Commission's opinion, such processing violates or is likely to violate Sections 24 (principles of personal data processing) and 25 (lawful basis of personal data processing) of the Act.
Establishment of the Nigeria Data Protection Commission and its Governing Council & Transitional Provisions Section 4 & 64	The Act establishes a Commission tasked with the responsibility of overseeing the provisions of the Act as well as issues related to data protection and privacy.	The establishment of this Commission is commendable and worthy of note is the fact that the Act has a transitional provision, which means that all powers and duties of the previously existing Nigeria Data Protection Bureau are transferred to the Commission.
Introduction of Legitimate Interest as a basis for processing personal data Section 25(1)(v)	The Act introduces legitimate interest of a data controller as one of the lawful bases for processing personal data. However, "legitimate interest" will not be a basis for processing personal data where such interests are overridden by the data subject's fundamental rights and freedom or are incompatible with the other lawful bases or the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.	The introduction of legitimate interest as a ground for processing data provides a lawful alternative for data controllers to process personal data. In addition, the Act introduces a balancing test for determining legitimate interest. Hence, the expectation is that such legitimate interest must be balanced with the fundamental rights and freedoms of the data subjects, etc. This is the standard test recommended by the United Kingdom's Information Commissioner's Office (ICO).

Exclusion of Definition of Legitimate Interest Section 25	Although the Act, mentions legitimate interest as a basis for processing data. It does not define the phrase. It is therefore unclear what the scope of legitimate interest is to invoke its applicability. The Act however, streamlines the scope of the meaning of legitimate interest in order to protect the fundamental rights of data subjects.	We recommend that subsequent amendments of the Act should include a definition for "legitimate interest" in such a way that mirrors processing of data for the legitimate interest of a business. The importance of defining the phrase is to prevent possible abuses of the rights of data subjects.
Data Privacy Impact Assessment Section 28	The Act provides that where the processing of personal data may likely pose a high risk to the rights and freedoms of data subjects, data controllers are required to conduct a data privacy impact assessment (DPIA). Where the DPIA indicates that the processing would result in a high risk to the rights and freedoms of a data subject, the data controllers are to consult with the Data Protection Commission prior to processing	The conduct of a data privacy impact assessment for processing activities that are likely to result in a high risk to the rights and freedoms of data subjects is already an existing obligation for data controllers under the Nigeria Data Protection Regulation (NDPR).. However, data controllers should take note of the new requirement to consult with the data protection commission in the event that the DPIA indicates that the processing would result in a high risk to the rights and freedoms of data subjects. It should however be noted, that the Act does not prescribe any specific number of days for the Commission to respond to the data controller. The Commission is also empowered to issue regulations and directives in respect of the foregoing.
Obligations of Data Controllers and Processors Section 29	Where a data controller or processor engages the services of another data processor, the data controller or processor should ensure that the engaged data processor – • Complies with the provisions of the Act as applicable to the data controller; • Assists the data controller/processor by the use of appropriate technical and organisational measures; • Implements appropriate technical andorganisational measures to ensure security, integrity and confidentiality of personal data; • Provides the data controller/processor with information reasonably required to comply and demonstrate compliance with the Act; • Notifies the data controller/processor when a new data processor is engaged; • Enters into a written agreement between the engaging data controller/processor.	These obligations are currently existing under the NDPR and the NDPR Implementation Framework and have now been codified in the Act. This provision is very relevant to companies that engage with vendors and other third parties. The vendors are effectively data processors that must comply with this provision. It is important for organisations to execute Data Processing Agreements and reserve the right to audit the data processes of their vendors, in order to ensure total compliance.

Sensitive Personal Data - Definition Section 30 / 65	Sensitive personal data is defined to mean personal data relating to genetic/biometric data, race or ethnic origin, religious or philosophical beliefs, health status, sex life, political opinions, trade union membership and other information prescribed by the Commission as sensitive personal data.	This definition is largely similar to what is contained in the NDPR. However, the Act does leave the list open ended and specifically empowers the Commission to prescribe additional categories of sensitive personal data as required.
Sensitive Personal Data Section 30	The Act lists out conditions for the processing of sensitive personal data as follows: • Where the data subject has given and not withdrawn consent for the processing activity; • Where the processing is necessary for the performance of the data controller's obligations or the existing rights of the data subject under employment or social security laws or any other similar laws; • Where the processing is necessary to protect the vital interests of the data subject or another person; • Where the processing is carried out by a non-profit organisation with charitable, educational, literary, artistic, philosophical, religious, or trade union purposes in the course of its legitimate activities provided that the processing relates solely to members of, former members of or persons who have regular contact with the entity in connection with its purpose. Furthermore, such sensitive personal data should not be disclosed outside of the entity without the explicit consent of the data subject; • Where the processing is necessary for reasons of substantial public interest on the basis of a law; • Where the processing is carried out for purposes of medical care or community welfare and undertaken by or under the responsibility of a professional owing a duty of confidentiality; • Where the processing is necessary for public health; • Where the processing is necessary for archiving purposes in the public interest on the basis of a law.	The introduction of the conditions for processing personal data has provided additional clarity on the administration of sensitive personal data in Nigeria. It is important for data controllers to take note of these conditions to ensure compliance with the provisions of the law. All the bases of processing personal data mostly apply to the processing of sensitive data – except contract. Data Controllers can however rely on the basis of performing the obligations under an employment contract, to process sensitive personal data. Otherwise, under no other circumstance can contract be relied upon as a basis to process sensitive personal data of a data subject. Data Controllers therefore need to review their existing processes to ensure that they have appropriate legal bases for processing any sensitive personal data within their custody as any processing of sensitive personal data for contract purposes (except employment) would be a breach of the provisions of the Act.

Children or person's lacking legal capacity to consent Section 31 / 65	The Act provides that where the data subject is a child or a person lacking legal capacity to consent, a data controller is required to obtain the consent of the parent or the legal guardian of the data subject and also apply appropriate mechanisms to verify the age and consent. The above consent will however not be required where the processing is: • Necessary to protect the vital interest of the child or person lacking the legal capacity to consent; • Carried out for purposes of education, medical or social care undertaken by or under the responsibility of a professional with a duty of confidentiality; • Necessary for proceedings before a court relating to the individuals. Furthermore, the Commission is empowered to make regulations for circumstances that relate to the processing of personal data of a child of 13 years and above by electronic means at the specific request of the child.	The introduction of specific provisions that deal with children or person's lacking capacity to consent is a welcome development as it provides additional clarity in this regard. There may be lack of clarity about the age of consent under the Act. Section 31(5) seems to suggest that a child above 13 can consent to processing of his/her personal data (The Commission can make regulations in this regard). Section 65, however, ascribes the definition of a child to that under the Child Rights Act which is persons below 18 years of age. For consistency and clarity, it is important that the Commission clarifies the age of legal capacity to consent as either 13 or 18. We await further guidance and clarification from the Commission in this regard.
Data Protection Officers Section 32	The Act mandates a data controller of major importance to designate a Data Protection Officer (DPO) with expert knowledge of data protection law and practices and the ability to carry out the tasks prescribed under the Act and its subsidiary legislation.	Under the NDPR, data controllers have an obligation to designate appropriate Data Protection Officers to ensure compliance with the data protection laws. The Act, however, appears to restrict the appointment of DPOs to only data controllers of major importance. The definition of data controllers/processors of major importance under the Act grants the Commission the discretion to determine the applicable threshold for qualification as data controllers/processors of major importance. We await further guidance on this to determine the extent of the compliance obligations of data controllers in this regard.
Data Protection Compliance Services Section 33	The Act empowers the commission to grant licenses to persons having requisite level of expertise in relation to the Act to monitor, audit and report on compliance by data controllers and processors.	Duly licensed Data Protection Compliance Organisations (DPCOs) already exist by virtue of the NDPR. It is therefore important for stakeholders to take note of the inclusion of data protection compliance services in the Act. In addition, the transitional provisions under Section 64 of the Act ratifiy all previously existing licenses and regulations issued by the National Information Technology Development Agency (NITDA) and the Nigeria Data Protection Bureau (NDPB). Based on the foregoing, DPCOs will continue to function in line with the provisions of the NDPR and the Act.

Rights of Data Subjects Section 34 - 38	The Act provides for specific rights of data subjects as follows: right to access, right to information, right to rectification, right to erasure, right to lodge a complaint with the commission, right to restriction of/objection to data processing, right to withdraw consent, right to object to a decision based solely on automated processing of personal data.	The rights of data subjects as provided under the Act are largely similar to the rights contained in the NDPR. It is important for data controllers, data processors and data subjects to take note of these rights.
Automated Decision Making (Section 37)	The Act outlaws data processors from automated decision making based solely on automated data processing. Subsection (2) makes some exceptions which are three in number: Contract, Legal Backing, Consent.	This provision is commendable. It is an attempt to ensure human intervention in personal data processing in order to safeguard the fundamental rights of data subjects.
Personal Data Breaches Sections 40(1)	Where a personal data breach occurs, with respect to personal data being stored or processed by a data processor, the data processor is obligated to notify the data controller. The data controller is required to assess the risk level of the breach to determine if it is likely to result in a risk to the rights and freedoms of the affected data subjects. If in the opinion of the data controller, it is likely to result in a risk, the data controller is to notify the Commission of the breach within 72 hours of becoming aware of the breach. On a separate note, where the breach is likely to result in a ***high*** risk to the rights and freedoms of a data subject, the data controller is required to immediately communicate same to the data subject.	Organisations are advised to take note of the wording of this provision, which is precise. The Act differentiates between a data processor and a data controller. Furthermore, the Act imposes separate obligations on the processor and controller. In summary, the processor is answerable to the controller. Additionally, there is a distinction between what constitutes 'risk' and 'high risk'; both of which are to be determined by the data controller. The obligation to report personal data breaches is more restrictive than what obtains in the NDPR. The data controller is mandated to report breaches that could result in 'risk' to the Commission. Whereas, the obligation to report to the data subject is restricted only to when the said breach is likely to result in '***high*** risk' to the rights and freedoms of a data subject.
Basis for cross-border transfer of personal data Section 41 - 42	This section prohibits data controllers/processors from transferring personal data to other jurisdictions unless the recipient of the personal data is subject to a framework that affords an adequate level of protection of personal data in line with the provisions of the Act. The Commission is also empowered to issue guidelines with respect to the assessment of adequacy and may approve Binding Corporate Rules, Codes of Conduct, contractual clauses or certification mechanisms proposed to it.	The provisions on cross border transfer of personal data bear large similarities to the existing provisions under the NDPR and NDPR Implementation Framework. Data controllers/processors should however take note of the powers of the Commission to review and approve documents for the purposes of ascertaining adequate protection of personal data. The Commission is also empowered to determine whether a country, region or specified sector within a country or standard contractual clauses affords an adequate level of protection.

Basis for cross-border transfer of personal data (contd.) Section 43	In the absence of an adequacy of protection in the transferee jurisdiction, a data controller/ processor may proceed to transfer personal data to such country if the: • Data subject has provided and not withdrawn consent to such transfer after being informed of the possible risks; • Transfer is necessary for the performance of a contact; • Transfer is for the sole benefit of the data subject and it is not reasonably practicable to obtain consent or the data subject would likely give consent; • Transfer is necessary for public interest; • Transfer is necessary for an establishment of legal claims; • If the transfer is necessary to protect vital interests	This provision provides clear details on circumstances where a data controller/ processor may proceed to transfer personal data to countries that do not have an adequate level of protection with respect to personal data.
Registration of data controllers and data processors of major importance Section 44	Section 44 creates the obligation for data controllers and data processors to register with the Commission within six months after the commencement of the Act or becoming a data controller or data processor of major importance. The Commission is also empowered to prescribe fees or levies to be paid by data controllers or processors of major importance and publish a register of duly registered data controllers and processors of major importance on its website.	The Act defines data controller/processors of major importance as; *"a data controller or 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 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".* Based on the foregoing definition, it would appear that a number of companies that already have compliance obligations under the NDPR may be classified as data controllers/processors of major importance for the purpose of registration with the Commission. However, we still await the guidance of the Commission with respect to the specific applicable threshold for qualification as data controllers/processors of major importance.
Registration of data controllers and data processors of major importance – Information to be provided Section 44	The registration of data controllers and processors of major importance would require such data controllers and processors to notify the Commission of the following: • The name and address of any representativeof any data processor operating directly orindirectly on its behalf; • A description of personal data and the categories and number if data subjects to which the personal data relate; • The purposes for which personal data is processed • The categories of recipients to whom the data controller or data processor intends or is likely to disclose personal data;	These are newly introduced compliance obligations that data controllers and processors should take note of. Hence, in addition to the 6 month timeline for registration, data controllers and processors should take note of the 60 day timeline in notifying the Commission of any significant change to information already submitted.

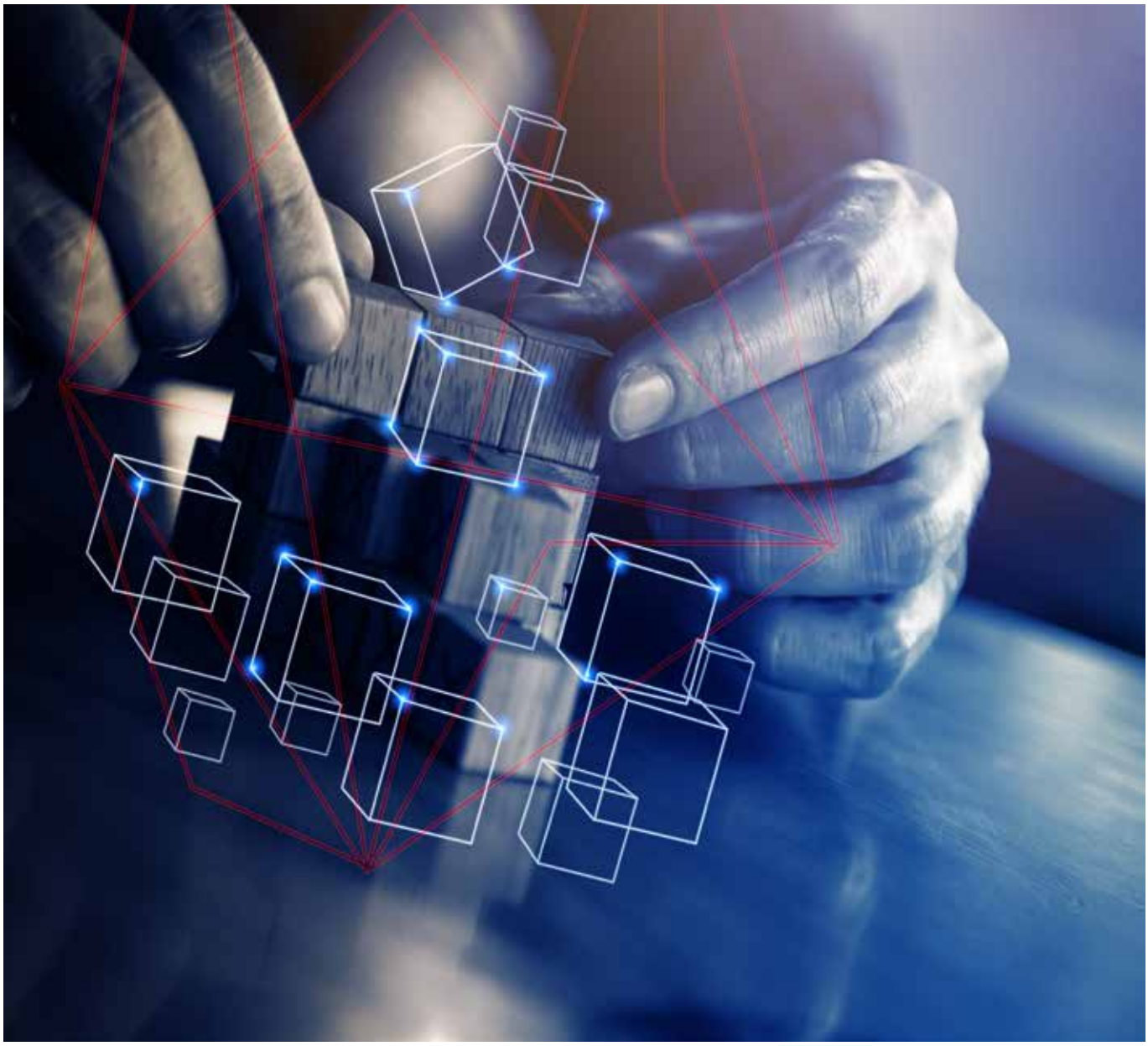
Registration of data controllers and data processors of major importance – Information to be provided (contd.) Section 44	• The name and address of any representative of any data processor operating directly or indirectly on its behalf; • The country to which the data controller or data processor intends, 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. Where there is any significant change to the information provided above the data controller or data processor of major importance are to notify the Commission within 60 days after such change.	
Complaints and Investigations, Compliance Orders Section 46 - 47	This section provides for the investigation of complaints made to the Commission by aggrieved data subjects. The Commission is also required to establish a unit to receive and follow up on complaints from data subjects and conduct investigations. When the Commission is satisfied that there has been a case of non-compliance by a data controller/processor the Commission may issue a Compliance Order to such processor which may include a warning, a requirement to comply or a cease and desist order. The Order shall also include the specific measures to be taken by a data controller/processor to avoid, remedy or eliminate the situation, a period within which to implement the measures and the right to judicial review.	The establishment of an outlined procedure for making and investigating complaints at the Data Protection Commission is commendable. This provision bridges the gap to justice, for data subjects whose privacy rights have been violated.
Enforcement Orders, Offences and Penalties (Sections 48 and 49)	Where the Commission is satisfied that there has been a case of non-compliance after conclusion of an investigation, the Commission may make any appropriate enforcement order or impose a sanction on the data controller or processor. The enforcement order will require the data controller/processor to: remedy the violation, pay compensation to a data subject who has suffered as a result, account for the profits realised from the violation; or pay a penalty or remedial fee. The penalty/remedial fee for non-compliance may be an amount up to: • The greater of ₦10million and 2% of the organisation's annual gross revenue in the preceding financial year in the case of a data controller/processor of major importance; or • The greater of ₦2million and 2% of the organisation's annual gross revenue in the preceding financial year in the case of a data controller/processor not of major importance.	It is important for organisations to take note of the possible penalties for non-compliance. Furthermore, the Data Protection Act now recognises the payment of compensation directly to a data subject as a possible penalty for a violation. This provision was previously not included in the NDPR.

Powers to Hear Data Protection Matters & Liability Sections 50 - 53	The Act vests powers in the courts to entertain judicial review of orders, within 30 days of issuance by the Commission. Data subjects can institute independent civil proceedings to recover damages, where the said data subject suffers injury, loss or harm. The Court may also make an order of forfeiture against a convicted data controller, processor or individual in accordance with the Proceeds of Crime (Recovery and Management) Act. Furthermore, where an offence has been committed by a body corporate or firm, the body corporate or firm as well as its principal officers shall be deemed culpable unless the principal officers prove that the offence was committed without their consent or connivance and they exercised diligence to prevent the commission of the offence. Data controllers and processors will also be vicariously liable for the acts or omissions of their agents or employees.	It is important for data controllers, processors and subjects to take note of these provisions. Organisations should endeavour to deploy extra efforts in conducting due diligence on their agents and other third parties to ensure strict compliance with the data protection laws. More so, employees should be adequately sensitised on the requirements of the data protection laws in order to prevent undue exposure of the organisation to non-compliance. Principal officers, which include management staff of the organisation should pay more attention to data protection compliance in their organisations as they can be held personally liable in the event of non-compliance of the organisation.
Priority of the Act Section 64	Where the provisions of any data processing law or enactment is inconsistent with any provisions of the Act, the provisions of the Act will prevail.	This Section provides for the clear supremacy of the Data Protection Act over other data protection laws in Nigeria such as the NDPR, the NDPR Implementation Framework and other Regulations and Codes of Conducts on data processing and data protection previously issued. It is however important to note that the Act does not repeal such prior legislation, However, where there is a discrepancy or inconsistency between the Act and any other previous Act or Regulation, the provisions of the Act will prevail.
Transitional Provisions Section 64	This Section continues the lifespan of any regulation, license or order issued by the erstwhile NDPB and NITDA , until such regulation, license or order is repealed, replaced, reassembled or altered.	The Act essentially lends life to the NDPR until the National Commissioner replaces it with another regulation. Additionally, the organisations licensed by the NDPB will remain so licensed, as if such licenses were issued by the Commission itself.

Conclusion

The enactment of the Nigeria Data Protection Act is a welcome development that is long overdue. Prior to the signing of the Act, many stakeholders had queried the legitimacy of the NDPR on the basis of the absence of a clear statutory provision or enabling Act. However, the Nigeria Data Protection Act now provides an unmistakable statutory basis for privacy law and practice in Nigeria.

Data controllers and processors are advised to engage their consultants with respect to the implications of the newly signed Act and how it may affect their business operations and day to day activities to ensure full compliance and avoid exposure to liabilities for non-compliance.



For comments and questions, please contact:

Michael Ango
Partner
Tax Advisory & Regulatory Services
E: michael.ango@ng.andersen.com

Samuel Ibrahim
Senior Manager
Tax Advisory & Regulatory Services
E: Samuel.Ibrahim@ng.Andersen.com

Emmanuel Omoju
Senior Manager
Tax Advisory & Regulatory Services
E: Emmanuel.Omoju@ng.Andersen.com

Patience Aliu
Manager
Tax Advisory & Regulatory Services
E: Patience.Aliu@ng.Andersen.com

Lagos, Nigeria

47 Glover Road, Ikoyi.
t: 0913 800 7000
(+234) 700TAXADVISERS

Abuja, Nigeria

Yobe Investment House, Suite 302,
Plot 1332 Ralph Shodeinde Street,
Central Business District, Abuja.

info@ng.andersen.com
marketing@ng.andersen.com

ng.Andersen.com

ng.Andersen.com/socialmedia