Jackson, Etti & Edu

OVERVIEW OF THE NEW NIGERIAN DATA PROTECTION ACT 2023

WWW.JEE.AFRICA

In today's digital age, where substantial volumes of personal information are generated, stored, and processed by businesses, the need for robust data protection measures is more critical than ever. Governments around the world are enacting legislation to regulate the handling of personal data and safeguard the privacy rights of individuals.

Nigeria's only response to data privacy issues was initially a reference to the constitutional right to privacy, as enshrined in section 37 of the Constitution. In 2019, the National Information Technology Development Agency (NITDA) introduced the Nigeria Data Protection Regulation (NDPR), which became the accepted legal framework for data protection in Nigeria, together with the NDPR Implementation Framework 2020. The issues of data protection, however, deserve a more formal legislative codification rather than a regulation, hence the need for a comprehensive Act of Parliament that would be enforceable in all superior courts of record in Nigeria.

On the 12th of June 2023, President Bola Ahmed Tinubu signed into law, the Nigerian Data Protection Act (NDPA). The Act aims to strike a balance between promoting innovation and protecting the privacy rights of individuals. It establishes a framework for organizations to handle personal data transparently, securely, and lawfully. By enacting this legislation, the government seeks to empower individuals by giving them control over their personal information and ensuring that businesses and organizations act responsibly when collecting, storing, and processing data.

This article highlights some of the key provisions of the NDPA. By examining these provisions, insights will be gained into the obligations placed on data controllers and processors, the role of the statutory regulator (the Nigerian Data Protection Commission) and the consequences of non-compliance.:

PART I

1. **Objectives and Application:** The Act sets out to safeguard the fundamental human rights of Nigerians as guaranteed by the 1999 Constitution of the Federal Republic of Nigeria, by regulating the processing of personal data, promoting practices which safeguard data security and privacy, ensuring fair and lawful processing of personal data, protecting data subjects' rights, and establishing a regulatory commission for data protection. It also emphasizes strengthening the legal foundations of the national digital economy and facilitating Nigeria's participation in regional and global economies through the trusted use of personal data.[1]

2. **Scope of Application:** The Act applies to the processing of personal data, whether automated or not. It applies when the data controller or data processor is based in Nigeria, the processing occurs within Nigeria, or if the personal data of a Nigerian data subject is processed by an entity outside Nigeria.[2] The purport of this is that the data processing activities of foreign or multinational companies that are not based in Nigeria but process personal data of Nigerians who are in Nigeria will be answerable to the Act. It would thus appear that the personal data of Nigerians who are not resident in Nigeria, are not within the scope of the Act.

3. **Exceptions:** The Act provides exceptions to its application. It does not apply to the processing of personal data carried out solely for personal or household purposes.[3] Additionally, certain obligations under Part V on Principles and Lawful Basis Governing Processing of Personal Data (other than sections 24,[4] 25[5], 32,[6] and 40[7]) of the Act do not apply to data controllers or processors, if the processing is carried out by a competent authority for specific purposes such as criminal investigation, public health emergencies, national security, journalism, or legal claims.[8] The Commission has the authority to exempt certain types of personal data and processing through regulations. The Commission can also issue guidance notices to data controllers or processors regarding exempted processing that may violate certain sections of the Act.[9]

PART II

4. **Establishment of the Nigeria Data Protection Commission:** The provision establishes the Commission as a corporate body which has perpetual succession and legal capacity. It can sue and be sued in its corporate name and has the power to acquire and dispose of

[1] Section 1
[2] Section 2
[3] Section 3(1)
[4] Section 24 of the Act provides the principles of personal data processing
[5] Section 25 provides for the Lawful basis of personal data processing
[6] Section 32 provides for the requirements of Data Controllers and Data Processors to have Data Protection Officers
[7] Section 42 expatiate on what to do when there is a personal data breach, requirements for reporting the breach and handling the breach
[8] Section 3(2)
[9] Section 3(3)

property.[10] The Commission is required to have its head office in the Federal Capital Territory and may establish other offices within Nigeria.[11]

The purport of sections 4 - 8 of the NDPA is that the Commission has become the specialized body empowered to administer and enforce the provisions of the Nigerian Data Protection law. Although the Act did not specifically mention the establishment of the position of the National Commissioner, that position was created by specific reference to the term 'the National Commissioner' as the driver of the Commission and a member of the Governing Council.

Furthermore, because the commencement date of the Act is not retrospective and there are lingering issues about the validity of the powers of the defunct National Data Protection Bureau (NDPB) and the National Commissioner, the Act in section 64 rectifies the position and provisions of the defunct NDPB. The Act also makes provisions for the appointment of the Governing Council by the President, including the National Commissioner, who is a member of that Council.

5. **Independence of the Commission:** The provision states that the Commission shall be independent in the discharge of its functions under the Act.[12] The Commission is mandated to develop and enforce regulations, codes, guidelines, and procedures to regulate its operations and fulfil its functions.[13] These regulations cover various aspects, including the conduct of the Commission's business, fostering accountability, transparency, and adherence to ethical standards. They also govern the budgeting and expenditure of the Commission, establish a governance code, define a code of conduct for the Commission's members and staff, and address any other relevant matters as directed by the Commission. This provision ensures that the Commission operates autonomously and in accordance with international best practices in data protection and privacy regulation.[14]

6. **Functions and Powers of the Commission:** The Commission is tasked with various activities to enhance personal data protection and ensure compliance with the Act. These include deploying technological and organizational measures for data protection, promoting awareness of obligations among data controllers and processors, and raising public awareness of personal data protection and associated risks. The Commission is also responsible for fostering the development of data protection technology, participating in international forums, receiving and investigating complaints, evaluating cross-border data transfers, ensuring compliance with standards and international agreements, registering important data controllers and processors, licensing compliance bodies, collaborating with relevant entities, collecting and publishing information on data protection, advising the government on policy matters, proposing legislative amendments, and implementing the

[10] Section 4(2)
[11] Section 4(3)
[12] Section 7
[13] Section 5
[14] Section 5(b)

Act's provisions. These provisions empower the Commission to regulate, enforce, and promote personal data protection in Nigeria.[15]

The provision grants the Commission various powers, such as overseeing the implementation of the Act, prescribing fees for data controllers and processors, issuing regulations, rules, directives, and guidance, determining filing requirements for data controllers and processors, conducting investigations into violations, imposing penalties for violations, acquiring, and disposing of assets, and performing other acts necessary for carrying out its functions. It can hire and license consultants to assist in fulfilling its functions when necessary.[16]

The arguments about the powers of the defunct Nigeria Data Protection Bureau (NDPB) vis-à-vis the powers of NITDA have therefore been laid to rest by the provisions and powers of the Commission. Furthermore, the supplementary provisions, retains the NITDA issued regulations and other actions by the NDPB.

PART III

7. **The Governing Council of the Commission** The Act establishes the Governing Council of the Commission and defines its composition, roles, and responsibilities.[17] The Council consists of members such as a retired judge, as the Chairman, the National Commissioner, representatives from relevant ministries and sectors, and a private sector representative.[18] The President appoints the National Commissioner and other Council members.[19] The Council oversees policy direction, approves plans and reports, sets terms of service, and provides advice to the National Commissioner. It may delegate responsibilities to committees.[20] The National Commissioner is responsible for executing the Commission's powers, implementing Council decisions, managing operations, appointing staff, and performing other necessary functions.[21]

   The Act also provides that part-time members of the Council will serve for four years and can be reappointed for another four-year term.[22] They will receive reasonable remuneration and allowances as determined by the collaboration with the Revenue Mobilization Allocation and the Fiscal Commission.[23] A person cannot be appointed or remain a member of the Council if they have undischarged bankruptcy, have been convicted of a felony or dishonesty offence, certified medically unfit, guilty of serious misconduct, or disqualified from practising their profession.[24] Members can resign by giving two months' notice[25], and the President can remove a member if they are disqualified.[26] If a member vacates office, the President will appoint a replacement for the remainder of the term.[27] Council members have fiduciary

[15] Section 5 (a-i)
[16] Section 12
[17] Section 8(1)
[18] Section 8(1) (a-d)
[19] Section 9(1)
[20] Section 12
[21] Section 14
[22] Section 10
[23] Section 8(2)
[24] Section 11 (1) (a-e)
[25] Section 11 (1) g
[26] Section 11(2)
[27] Section 11(3)

duties, must avoid conflicts of interest, and disclose any personal interests.[28] They cannot make secret profits or accept gifts that may impair their impartiality.[29] Violations can result in fines and imprisonment: a fine of not less than N 10,000,000:00 or imprisonment for a term of up to three years, or both.[30]

The Council plays a vital role in guiding the Commission, ensuring diverse expertise and effective governance. The National Commissioner leads the Commission's operations, executing policies and decisions, and manages day-to-day affairs.

PART IV FINANCIAL PROVISION

8. Funding for the Commission

The Act establishes a Fund for the Commission, from which all its expenses will be covered.[31] The Act specifies the percentages and sources of the take-off grant, as well as the types of expenses that will be chargeable to the Fund. The Council will manage the Fund according to established rules. These provisions ensure that the Commission has the financial resources to carry out its functions and responsibilities effectively.[32]

The clear allocation of funding sources and percentages aims to diversify and distribute financial support, fostering collaboration and partnerships between various government entities. However, the Act does not provide specific details on the budgetary process, transparency mechanisms, or oversight of the Fund, which could impact financial accountability and control. Further clarity on financial management, accountability mechanisms, and reporting requirements would enhance transparency and oversight in line with international best practices.

The Act specifies the expenses that will be chargeable to the Fund established under Section 20. These include approved expenses of the Commission, repayment of borrowed funds, allowances and remuneration for Council members and staff, administrative costs, contract payments, capital expenditure, investments, and other necessary expenditures for the Commission's functions. The Fund will be managed according to rules established by the Council. The Act grants the Commission the authority to borrow money when necessary to fulfil its functions. It also allows the Commission to accept gifts, grants, aids, or other property that align with its objectives and functions, subject to certain terms and conditions.[33]

Scholars have raised concerns towards allowing Government agencies the power to borrow money and accept gift items. Often, this could lead to abuse and make it extremely impracticable for successors to function optimally.

[28] Section 13(1)
[29] Section 13(1) (b)
[30] Section 13 (2)
[31] Section 19(1)
[32] Section 19(2)
[33] Section 21

PART V ANNUAL ACCOUNT

9. Annual Accounts of the Commission

The provisions state that the Commission is required to keep proper accounts and records for each financial year and have them audited within six months after the end of the year.[34] The financial year of the Commission is typically from 1st January to 31st December, but it can be determined differently by the Council.[35] The accounts of the Commission will be audited by an independent firm of auditors approved by the Auditor-General for the Federation.[36] The Commission must prepare and submit a report to the National Assembly within six months after each financial year, which includes the activities of the Commission and its audited accounts.[37] Additionally, the Commission is required to prepare and present a statement of estimated income and expenditure for the next financial year to the National Assembly, and can also submit supplementary or adjusted statements if needed.[38]

PART VI - PRINCIPLES AND LAWFUL BASIS GOVERNING PROCESSING OF PERSONAL DATA

10. Overview of Principles of Data Processing

The Act establishes the principles and lawful basis governing the processing of personal data. It states that data controllers and processors must ensure that personal data is processed fairly, lawfully, and transparently. Personal data should be collected for specified purposes and not further processed in a way incompatible with those purposes. It should be adequate, relevant, and limited to the minimum necessary. Data should be retained for no longer than necessary and should be accurate, complete, and kept up to date. Processing should ensure appropriate security measures to protect against unauthorized access, loss, or damage. Data controllers and processors must demonstrate accountability and bear the duty of care in data processing.

11. Lawful Basis of Personal Data Processing

The Act outlines the lawful bases for personal data processing. It states that processing is lawful if the data subject has given consent, if it is necessary for the performance of a contract or legal obligation, to protect vital interests, for tasks in the public interest or official authority, or legitimate interests pursued by the data controller or a third party.[39] It also specifies conditions under which interests are not considered legitimate. They are as follows; (a) they are overridden by the fundamental rights and freedoms and the interests of the data subject; (b) they are incompatible with other lawful bases of processing under

[34] Section 22(1) (a-c)
[35] Section 22(1-4)
[36] Section 22(2)
[37] Section 23(1)
[38] Section 23(2)
[39] Section 25(1)

subsection (1)(b) of this section; or (c) the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.[40]

12. Conditions of Consent

The Act places the burden of proof on the data controller to establish the data subject's consent. It clarifies that consent must be freely and intentionally given and that silence or inactivity does not constitute consent. Data subjects have the right to withdraw consent, but the withdrawal does not affect the lawfulness of prior processing. Silence or inactivity shall not be regarded as consent. Consent can only be affirmative, not based on pre-selected confirmations (that is the option shall not be ticked before showing it to the data subject).[41]

13. Provision of Information to the Data Subject

The Act requires data controllers to inform data subjects of their identity, purposes of the processing, recipients of data, data subject rights, the right to lodge complaints, and the existence of automated decision-making. This information must be provided before collecting data directly from the data subject unless it is impossible or involves disproportionate effort.[42]

14. Data Protection Impact Assessment

The Act introduces the requirement for a data protection impact assessment (DPIA) when processing personal data that poses a high risk to data subjects' rights and freedoms. The data controller must carry out a DPIA and consult the Commission if necessary. The Commission is saddled with the responsibility of issuing guidelines and directives for this process.[43]

15. Obligations of Data Controllers and Processors

The Act places obligations on data controllers and processors when engaging the services of another data processor. They must ensure compliance with principles, assist in fulfilling data subject rights, implement security measures, provide the necessary information, and notify the Commission of the engagement of new processors. This engagement of processors must be based on an agreement between data processors and data controllers[44]

16. Sensitive Personal Data[45]

The Act specifies the conditions for processing sensitive personal data. It lists various legal bases, including consent, legal obligations, protection of vital interests, legitimate activities, public interest, medical care, and archiving purposes.[46] The Commission can prescribe additional categories, grounds, and safeguards for sensitive data processing.[47]

17. Data of Children & Individuals lacking the capacity to consent

---

[40] Section 26(2)
[41] Section 26
[42] Section 27
[43] Section 28
[44] Section 30
[45] Section 65 (Interpretation section) 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) any other personal data prescribed by the Commission as sensitive personal data pursuant to section 31(2)
[46] Section 30(1) (a-i)
[47] Section 30(2)

The Act addresses the processing of personal data concerning children or individuals lacking the legal capacity to consent. It requires obtaining consent from a parent or legal guardian, with appropriate mechanisms for age verification. Exceptions apply in certain circumstances.[48]

18. **Data Protection Officers**
    The Act mandates that data controllers of major importance designate a data protection officer (DPO) to advise on data protection obligations, monitor compliance, and act as a contact point for the Commission.[49]

19. **Data Protection Compliance Services**
    The Act grants the Commission the authority to license bodies or individuals with expertise in data protection to monitor and report on compliance by data controllers and processors with the Act and related codes of conduct.

PART VII - RIGHTS OF A DATA SUBJECT

20. **Right to be informed:** This provision grants data subjects the right to obtain information from data controllers regarding the processing of their personal data. It includes details such as the purposes of the processing, categories of personal data, recipients of data, data retention period, rights to rectification or erasure, right to lodge a complaint, source of data, and the existence of automated decision-making. The NDPR 2019 does not explicitly outline these specific details but provides similar rights to data subjects.[50]

21. **Right to Data Portability:** This provision grants data subjects the right to receive a copy of their personal data in a commonly used electronic format, except when it imposes unreasonable costs on the data controller. The NDPR 2019 does not specifically mention the format of data copies but grants data subjects the right to access their personal data.[51]

22. **Right to Rectification:** This provision grants data subjects the right to correct or delete inaccurate, out-of-date, incomplete, or misleading personal data. The NDPR 2019 also provides similar rights to data subjects.[52]

23. **Right to Erasure:** This provision grants data subjects the right to request the erasure of their personal data if it is no longer necessary for the purposes it was collected or if the data controller has no other lawful basis to retain it. The NDPR 2019 provides a similar right to data subjects.[53]

24. **Right to Restrict Processing:** The Act grants data subjects the right to request the restriction of data processing while their request or objection is being resolved or for the

[48] Section 31
[49] Section 32
[50] Section 34
[51] Section 34(b)
[52] Section 34(c)
[53] Section 34(2)

establishment, exercise, or defence of legal claims. The NDPR 2019 also grants data subjects a similar right to restrict processing.[54]

25. **Withdrawal of Consent:** The Act grants data subjects the right to withdraw their consent to the processing of personal data at any time. It emphasizes that the withdrawal process should be as easy as giving consent.[55]

26. Right to Object to Processing Personal Data

Data subjects are granted the right to object to the processing of personal data based on specific grounds, including profiling. The data controller can only continue processing if there are public interest or legitimate grounds that override the rights and freedoms of the data subject.[56]

27. Automated Decision Making

Data subjects are also granted the right not to be subject to decisions based solely on automated processing, including profiling if it produces legal or similarly significant effects.[57] However, there are exceptions when automated decisions are necessary for a contract, authorized by written law with safeguards, or authorized by the data subject's consent.[58]

28. Obligation of the Commission regarding the Right of Data Portability

The Commission is empowered to establish rules for the right of personal data portability.[59] It grants data subjects the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit the data to another data controller.[60] The NDPR 2019 does not explicitly outline a right to data portability.

While some provisions introduce additional details and clarify certain rights compared to the NDPR 2019, the core principles remain consistent in safeguarding the rights of data subjects.

PART VIII

29. Data Security

The Data Protection Act focus on data security measures and personal data breaches. Data controllers and data processors are required to implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of personal data. These measures should protect against accidental or unlawful destruction, loss, misuse, alteration, unauthorized disclosure, or access. Factors such as the amount and sensitivity of the data, potential harm to data subjects, processing extent, data retention period, and available technologies should be taken into account. The Act suggests various measures, including pseudonymization, encryption, system and service security, data

[54] Section 34(e)
[55] Section 35
[56] Section 36
[57] Section 37(1)
[58] Section 37(2)
[59] Section 38(1)
[60] Section 39(2)

restoration processes, risk assessments, testing and evaluation, and regular updates to address evolving risks.[61]

30. Data Breaches

The Act addresses personal data breaches. If a breach occurs concerning personal data held or processed by a data processor, they must notify the data controller without delay. The data processor should describe the nature of the breach and provide relevant information to assist the data controller in meeting their obligations. In cases where the breach is likely to pose a risk to individuals' rights and freedoms, the data controller must notify the Commission within 72 hours. They should also communicate the breach to the affected data subjects, providing clear and concise information about the breach and advice on mitigating its effects. If direct communication with individuals is not feasible, public communication may be made. The Commission has the authority to make public communications about breaches if it deems the data controller's actions insufficient. Record-keeping requirements and the evaluation of risk factors are also included in these provisions.[62]

PART IX - CROSS-BORDER TRANSFERS OF PERSONAL DATA

31. Basis for Cross-Border Transfer of Personal Data

Data controllers or processors cannot transfer personal data from Nigeria to another country unless the recipient of the data offers an adequate level of protection through laws, binding corporate rules, contractual clauses, codes of conduct, or certification mechanisms. Alternatively, the transfer can take place if specific conditions outlined in Section 43 of the Act apply.[63] Data controllers and processors must maintain records of the basis for transferring personal data and the adequacy of protection.[64] The Commission has the authority to establish rules that require data controllers and processors to notify the Commission about the measures they have in place to ensure data security and explain their adequacy.[65] Additionally, the Commission can identify specific categories of personal data that have additional restrictions on transferring them to another country, taking into account the nature of the data and the risks to data subjects.[66]

32. Adequacy of Protection

The Act states that a level of protection is considered adequate if it upholds principles similar to those outlined in the Data Protection Act. When assessing adequacy, factors such as enforceable data subject rights, access to administrative or judicial redress, the existence of data protection laws, competent supervisory authorities, and international commitments are taken into account. The Commission is responsible for issuing guidelines and

[61] Section 39
[62] Section 40
[63] Section 41(1)
[64] Section 41(2)
[65] Section 41(3)
[66] Section 41(4)

determining whether a country, region, sector, or contractual provisions meet the requirements of adequacy.[67]

33. Other bases for Transfer of Personal Data outside Nigeria

In the absence of adequate protection, the Act outlines alternative bases for transferring personal data outside Nigeria. These include obtaining and maintaining the consent of the data subject, transfers necessary for the contractual performance or initiation, transfers in the data subject's interest, transfers for public interest reasons, transfers for legal claims, and transfers to protect vital interests when the data subject is unable to provide consent.[68]

PART X – REGISTRATION & FEES

35. Registration of Data Controllers & Processors of Major Importance

Data controllers and data processors of major importance must register with the Commission within six months of the Act's commencement or upon becoming a data controller or processor of major importance.[69]

Registration requires providing information such as the name and address of the controller or processor, the data protection officer's details, a description of personal data, purposes of the processing, recipients of data, security measures, and other required information.[70] Any change to the submitted information must be notified to the Commission within sixty days.[71]

The Commission shall maintain on its website a register of registered data controllers and processors of major importance.[72] The Commission may remove any controller or processor that notifies that it is no longer a controller or processor of major importance.[73] Exemptions from registration may be granted by the Commission for certain classes of controllers or processors.[74]

34. Fees

The commission has the authority to establish fees or levies that must be paid by data controllers and processors of major importance, and these fees can vary based on different classes of such entities as determined by the Commission.[75]

PART XI - ENFORCEMENT

36. Complaints and Investigation

Data subjects can lodge complaints with the Commission[76], which will investigate valid complaints that are not frivolous or vexatious.[77] The Commission has the power to initiate investigations on its

[67] Section 42
[68] Section 43
[69] Section 44(1)
[70] Section 44(2) (a-h)
[71] Section 44(3)
[72] Section 44(4)
[73] Section 44(5)
[74] Section 44(6)
[75] Section 45
[76] Section 46 (1)
[77] Section 46(2)

own if it suspects a violation has occurred or may occur.[78] It can order individuals to provide information, attend examinations, produce documents, and grant access to electronically stored information.[79] The Commission can make representations to the parties involved, establish a unit for handling complaints and investigations, and establish rules and procedures for the process.[80]

35. Compliance Orders

The Commission shall determine if a data controller or data processor has violated or is likely to violate any requirement under the Act, regulations, subsidiary legislation, or orders, after which it can then issue a compliance order. This order can include a warning about potential violations, a requirement for the entity to comply with specific provisions or data subject requests, or a cease-and-desist order to stop processing certain personal data. The order must be in writing and specify the violated provisions, measures to rectify the violation, a timeframe for implementation, and the right to judicial review if an actual violation has occurred.[81]

36. Enforcement Orders

The penalty for any violation can be up to the higher maximum amount for data controllers or processors of major importance, and the standard maximum amount for others, with the higher maximum amount being the greater of ₦10,000,000 or two per cent of their annual gross revenue derived from Nigeria in the previous financial year, and the standard maximum amount being the greater of ₦2,000,000 or two per cent of their annual gross revenue derived from Nigeria in the previous financial year. When determining the sanctions, the Commission considers factors such as the nature, gravity, and duration of the infringement, the purpose of the processing, the number of data subjects involved, the level of damage and mitigation measures taken, intent or negligence, cooperation with the Commission, and the types of personal data involved.[82]

37. Offences

A data controller or data processor who fails to comply with orders issued under section 49 of the Act commits an offence and is liable to a fine, which can be the higher maximum amount for entities of major importance or the standard maximum amount for others, as specified in section 47. They may also face imprisonment for up to one year or a combination of both.[83]

38. Judicial Review

The Act allows a person who is dissatisfied with an order made by the Commission to apply for judicial review within thirty days of the order being issued.[84]

39. Civil Remedies

A data subject who suffers injury, loss, or harm due to a violation of the Act by a data controller or data processor, or a recognized consumer organization acting on behalf of the data subject, has the right to seek damages through civil proceedings in the appropriate court against the responsible data controller or data processor.[85]

---

[78] Section 46(3)
[79] Section 46(4-5)
[80] Section 46(6-8)
[81] Section 47
[82] Section 48
[83] Section 49
[84] Section 50
[85] Section 51

40. Forfeiture

The Court[86] shall have the authority to order a convicted data controller or individual to forfeit assets to the Government by the Proceeds of Crime (Recovery and Management) Act or any similar law, with the Commission being recognized as a "Relevant Organization" for this purpose.[87]

41. Joint & Vicarious liability

Where an offence is committed by a corporate body or firm, the directors, managers, partners, secretaries, or similar officers of that entity are also deemed to have committed the offence unless they can prove that it was committed without their consent or connivance. They must demonstrate that they exercised due diligence to prevent the offence considering the nature of their functions and the circumstances. Additionally, the provision establishes vicarious liability for acts or omissions of agents, clerks, servants, or other individuals concerning the business of the data controller or data processor.[88]

PART XII – LEGAL PROCEEDINGS

No suit can be filed against the Commission, its officers, or employees unless it is commenced within three months of the act complained of, and a written notice of intention to sue is served upon the Commission.[89] Any required documents should be served by delivering them to the National Commissioner at the Commission's Head Office.[90] The Act prohibits the execution or attachment of the Commission's property in relation to a lawsuit, and any judgment awarded against the Commission must be paid from its Fund.[91] The Commission will indemnify its National Commissioner, officers, and employees against losses and liabilities incurred in the execution of their duties or in defending criminal or civil proceedings.[92]

The Act allows the Commission to apply for a warrant to obtain evidence in investigations related to the Act. A judge can issue a warrant if satisfied that certain conditions are met, granting the Commission authority to enter and search premises, seize evidence, and access and decrypt data.[93] The Act also permits the Commission's legal officers or engaged private practitioners to represent the Commission in civil proceedings pertaining to its business or operations.[94]

PART XIII - MISCELLANEOUS

The Commission is empowered to make regulations to fulfil its objectives under the Act. These regulations can cover various aspects such as financial management, personal data protection, the exercise of powers and duties by the Commission, prescribed matters, application forms, complaint procedures, fees, fines, and any other necessary measures to achieve the objectives of the Act. The

[86] Section 65 defines court as a High Court or Federal High Court.
[87] Section 52
[88] Section 53
[89] Section 54
[90] Section 55
[91] Section 56
[92] Section 57
[93] Section 58
[94] Section 59

regulations may also establish offences with penalties of fines not more than what is allowed by the Act. The Commission is required to publish on its website draft regulations and invite public comments before finalizing them.[95]

The Commission is empowered to make directives that will guide the operations of the commission, ensure accountability in the commission, guide the internal operations, and ensure ethical standards and compliance with international best practices.[96] The Act designates the Commission as the successor-in-title to the Nigeria Data Protection Bureau, encompassing its powers, duties, and functions. Existing staff, agreements, records, equipment, and documents of the Bureau become part of the Commission, ensuring continuity, and preserving applicable laws and arrangements until they are repealed or amended.[97]

CONCLUSION

In conclusion, the enactment of the Data Protection Act in Nigeria represents a significant step forward in safeguarding individuals' data rights. However, it is not solely the content of the Act that will shape its impact, but rather the enforcement of its provisions in the years to come. It is crucial for the Data Protection Commission to actively carry out enforcement actions, but even more significant is the role of the superior courts of records in interpreting the Act and expanding its jurisdiction. As such, data controllers and processors in Nigeria must seek legal guidance and collaborate with their appointed Data Protection Compliance Officers (DPCOs) to ensure full compliance with the law. By increasing awareness of data rights among Nigerians and encouraging litigation or reporting to the commission, the continuous relevance of the law can be maintained. Therefore, public enlightenment efforts should be prioritized to help individuals realize the data rights afforded to them by the Act. To truly accelerate the development of data protection and privacy in Nigeria, all stakeholders must take responsible action and actively contribute to the implementation of the Act.

Authors

Ifeanyi Okonkwo

Senior Associate, Deputy Sector Head, Technology, Media & Entertainment.

Adeyemi Owoade

Associate, Intellectual Property Department.

[95] Section 61
[96] Section 62
[97] Section 64

Jackson, Etti & Edu

Key Contacts

For further information, kindly reach the key contacts below:

NGOZI ADERIBIGBE

Partner, Head of Department,
Intellectual Property & Data Protection.

+234 1 4626841/3

E: ngozi.aderibigbe@jee.africa

Victoria Island

RCO Court,
3-5 Sinari Daranijo Street,
Victoria Island,
Lagos, Nigeria
island.

Tel

+234-1-4626841/3,
+234-1-2806989

Email

jee@jee.africa

Abuja

42, Moses Majekodunmi Crescent.
Utako, FCT, Abuja

Ikeja

1st floor, ereke house,
Plot 15, CIPM Avenue
CBD Alausa Ikeja
Lagos Nigeria

Accra

3 Emmause, 2nd Close
Akosombo House
Labone, Accra, Ghana
P.O. Box 14951
Accra, Ghana

Yaoundé

3rd Floor, Viccui Building
Apt. 15-16, Carr Street
New Town, Yaoundé
Cameroon

Harare

38 Clairwood Road,
Alexandra Park,
Harare,
Zimbabwe.