International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 13-08-2025, Accepted: 14-09-2025, Published: 29-09-2025
Volume 7, Issue 3, 2025, Page No. 128-132

Data processing principles and the rights of data subjects under the Nigeria data protection act 2023

George RC Ibekwe[1], Thomas O Okaba[2], Chukwu Arthur Elvis[2]
[1] Deputy Director Academics, Nigerian Law School, Victoria Island Lagos, Nigeria
[2] Depuy Director Academics Nigerian Law School Yola, Nigeria

Abstract
The world has become a global and technological village where personal data processing, storage and retrieval have become a very important and inevitable aspect of administrative and economic activities for both public and private organizations. This has impelled governments across the world, including Nigeria, to enact laws to protect natural persons whose personal data are collected, processed, stored and or retrieved. The laws establish certain rights for the data subjects and set out some basic data processing principles. The rights of data subjects relate to those entitlements or claims which the law sets out for the benefit of data subjects, which if breach constitutes an infringement on the data subjects' rights and entitles the data subject to remedies. While Data processing principles relates to the basic rules and doctrine which govern the processing of personal data of data subjects. Nigeria was lethargic in enacting her substantive law on data protection unlike her global counterparts and this was largely due to her lack of political will. However, after decades of consistent agitations and efforts by stakeholders, the Nigeria Data Protection Act was finally enacted in 2023. This article examined data processing principles and the rights of data subjects set out in the Data Protection Act 2023. It also discussed the measures to safeguard personal data. It recommends among others, that there should be a comprehensive and diligent implementation of the laudable rights of data subjects under the Act, and that Data controllers and processors should establish adequate data security measures to ensure that the rights of data subjects as enshrined in the Act are preserved and not infringed upon.

Keywords: Personal data, data subjects, dssata processing principles, rights of data subjects

Introduction

In an effort to regulate the processing of personal data in the country and to protect data subjects, the federal government of Nigeria issued the Nigerian Data Protection Regulations (NDPR) in 2019 [1]. This Regulation, although commendable, was highly criticized by many stakeholders for being bereft of the necessary legal biting tooth given that it is a mere regulation and lacking independent data protection authority to implement it. Consequently, the desire and pressure to have an Act of National Assemble regulating the processing of personal data and establishing an independent data processing commission was continually mounted by stakeholders.

On the background of the foregoing, several data protection bills were sponsored at both chambers of the national assembly at different times but, until 2023, all the previous bills were either not passed by both chambers of the national assembly or presidential assents were withheld. On the 12th day of June 2023, the president of the federal republic of Nigeria, His Excellency, Bola Ahmed Tinubu signed the Nigeria Data Protection Bill 2023 into an Act thereby giving Nigeria her first Data Protection Act. The new Act now substantively establishes the principles of personal data processing and the rights of data subjects amidst other provisions.

The Act defines personal data as any information relating to an individual which can be used directly or indirectly to identify the individual by reference to such information as name, identification number, address, physical, genetic, social, or cultural identity [1]. Whereas personal data processing refers to any operation or set of operations carried out on personal data such as collection, recording, storage, adaption, alteration, retrieval, use, disclosure, transmission, dissemination, combination, erasure, restriction or destruction.

The Act [1] did not define the term data processing principle. However, it can be seen as those principles relating to the basic rules and doctrine which govern the processing of personal data of data subjects. For the processing of personal data to be lawful, the set out basic rules and doctrine must be upheld by the data controller and data processor.

A data subject is 'an individual to whom personal data relates [1].' It is 'any person who can be identified, directly or indirectly by reference to an identification number of more factors specific to his physical, physiological, mental, economic, cultural or social identity.' [1] A data subject can also be seen as a natural person who is a subject of personal data processing [2].

Principle governing the processing of personal data

Section 24 of the Act [3] has clearly spelt out the principles that should govern the processing of personal data in Nigeria.

Section 24(1) provides thus:

A data controller or data processor shall ensure that personal data is –

a. Processed in a fair, lawful and transparent manner;
b. Collected for specific, explicit and legitimate purposes, and not be further processed in a way incompatible with these purposes;
c. Adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;

d. Retained for no longer than is necessary to achieve the lawful basis for which the personal data was collected or further processed;
e. Accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected, or further processed; and
f. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.

The above principles must be adhered to by all data controllers and data processors. Data controllers and data processor are under obligation to employ the necessary technical and organizational measures to ensure confidentiality, integrity and availability of personal data [4]. Under the Act, a data controller or data processor owes the data subject a duty of care and is accountable to the data subject for his acts or omissions in respect of the data [5].

Lawful processing of Personal Data

The Act requires the processing of personal data to be lawful. The processing must be fair and transparent [6]. The processing of data would be lawful if the data subject gives and did not withdraw consent for the processing of his personal data for specific purpose or purposes [7]; or where the processing is pursuant to a contract to which the data subject is a party; or the processing is in furtherance of a legal obligation to which the data controller is subject to; or it is in the public interest or for the purpose of protecting the right of another data subject or for a legitimate interest pursued by the data controller, data processor or any third party [8]. For the purpose of lawful processing of personal data, an interest would not be legitimate if it overrides the rights and interest of the data subject; it is incompatible with the lawful basis for processing personal data; or if the data subject would not have reasonably expected that his data would be processed in the manner it was processed or envisaged [9].

Specific Purpose

The collection, processing, storage and or retrieval of personal data shall be for specific, explicit and legitimate purposes. It is not sufficient to only specify the purpose, the purpose or purposes must be explicitly communicated to the data subject [10]. It is illegal for personal data to be further processed in a way incompatible with purpose for which it was initially processed. This principle will be breached if the data controller or data processor processes personal data without specifying and communicating the specific purpose for which the data is being processed.

Adequacy and Relevance

The processing of personal data must be adequate, relevant and restricted to the minimum data necessary for the purposes for which the data was processed or further processed [11]. It therefore follows that where the data is inadequate or not relevant to the purposes, the processing will be in breached of this principle. The data subject of an inadequately processed data is entitled to request the data controller or processor to make the data adequate in exercise of his right to correction or update of his data. The Act also prohibits the processing of data in excess of the purpose of such processing.

Retention for Longer Period than Necessary

This principle is against the storage and retrieval of personal data for a period longer than is it 'necessary to achieve the lawful basis for which the personal data was collected or further processed.' [12] Under this principle, data controllers and processors are required to delete or destroy personal data after achieving the purpose for which the data was processed.

Accurate and Complete Data

Here, the data controllers and possessors are obliged to ensure that personal data are accurate, complete and not misleading. The data is to be up to date and kept updated for the purpose for which it is processed or further processed.

Appropriate Security of Personal Data

Data controllers and processors have a responsibility to ensure that personal data is processed in such a way that guarantees security of the data. There should be a security network in place to protect against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach.

Rights of Data Subjects

The Act has established certain rights which data subjects are entitled. These rights include the following: [13]

1. Right to obtain confirmation from the data controller or data processor as to whether the personal data of a data subject is being processed or stored.
2. Right to know the category of personal data being processed.
3. Right to know the recipient or categories of recipients to whom the personal data have been or will be disclosed to.
4. Right to know the period and criteria used in the storage of the personal data.
5. Right to request from the data controller the rectification or erasure of personal data.
6. Right to request from the data controller the restriction of processing of personal data.
7. Right to request for information as to the source of the personal data if the data is not supplied personally by the data subject.
8. Right to obtain without delay, a copy of the data subject's personal data in commonly used electronic format with or without cost.
9. Right to correction or deletion of inaccurate, out of date, incomplete or misleading personal data.
10. Right to give and withdraw consent [14].
11. Right to object to the processing of personal data [15].
12. Right to data portability [16].
13. Right not to be subjected to a decision based solely on automated processing of personal data [17].
14. Right to lodge complaint at the Commission [18].

For personal data to be collected and/or processed, the collection and processing must be for a specific purpose and be consented to by the data subject. The consent shall be voluntarily given and or withdrawn at any time, devoid of fraud, coercion or undue influence [19]. The data controller

has an obligation to make it easy for data subjects to withdraw consent as it is to give consent.

Where a data subject is not in support of the processing of his data, it is his right to object to the processing of his personal data. Once an objection is made by the data subject, the data controller or processor shall cease to process the data [20]. However, if the data controller can show a legitimate ground or public interest which overrides the individual right of the data subject to object, it may continue the processing of the data notwithstanding the objection.

The right to data portability is not expressly conferred on data subjects by the Act. The Act instead empowered the Data Protection Commission to issue regulations establishing the right to data portability. The Act provides that 'the commission may make regulations establishing a right of personal data portability [21].' This right entitles the data subject to obtain from the data controller his personal data in a commonly used and machine-readable format and to transmit the data to another data controller. It also entitles the data subject to have his data transmitted from one data controller to another if it is technically possible. Subjecting this right to a blank check of 'technically possible' has been criticized as capable of being exploited by data controllers who may not be willing to transfer personal data to another data controller [22]. A data controller who is unwilling to transmit personal data to another may unjustly claim that it is technically impossible to do so.

Where the data processing process is automated, the data subject cannot be subject solely to the automated processing [22]. This is to prevent a situation where the data subject is faced with automated processing and decision taking which greatly affect the data subject [22]. The data subject has the right to express his point of view and to have a human intervention by the data controller [21]. While the Act allows automated processing of data and decision making, it however obliged data controller to put in place measures to safeguard data subjects' rights [18].

Judicial Interpretation

The rights of data subjects and the entire provisions of the Data Protection Act 2023 are yet to be tested in the furnace of judicial interpretation as the Act has just been signed into law. However, there are decisions from the Court of Justice of the European Union (CJEU) on the interpretation of the European Union General Data Protection Regulation (GDPR) which are not only persuasive but directional toward the interpretation of the Data Protection Act 2023. This is because the provisions of the Act are largely copied from the GDPR, and these decisions are of common law jurisdiction.

The CJEU while interpreting Article 15(1) (c) of GDPR dealing on the right of data subjects to request information on recipients, held thus:

Where personal data has been or will be disclosed to recipients, there is an obligation on the part of the controller to provide the data subject, on request, with the actual identity of those recipients. It is only where it is not (yet) possible to identify those recipients that the controller may indicate only the categories of the recipient in question [14].

In *FF v CRIF GmbH* [15] the CJEU, while interpreting Article 15(3) GDPR which requires controllers to provide data subjects with a copy of their personal data upon request, held that the data subject is entitled to a faithful and intelligible reproduction copy of his personal data. The CJEU however held that the data controller is not obliged to disclose any information not being the personal data of the data subject who is making the request; or any data beyond the scope of the request made by that data subject.

In *Case C-579/21 Pankki S*, [16] the CJEU held that 'the GDPR must be interpreted as meaning that information relating to consultation operations carried out on a data subject's personal data and concerning the dates and purposes of those operations constitutes information which that person has the right to obtain from the controller [30].'

In *UI v Österreichische Post A* [31] *G* the CJEU rejected the contention that Article 82(1) of the GDPR (dealing on right to compensation and liability) creates an automatic right to compensation once a controller violates the GDPR. It held that 'Article 82(1) of the GDPR must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation.' The Court emphasized that compensation can only be awarded where, the defendant violates the GDPR and the violation occasioned material or non-material damage suffered by plaintiff. This interpretation therefore placed a burden on the data subject to establish that he suffered injury as a result of the violation of his right before he can be entitled to the award of damages.

Breach of Rights of Data Subjects and Remedies

The breach of rights of data subjects occurs where the data controller or data processor breaches data security thereby leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data, or unauthorized use [32]. The data controllers and data processors are under obligation to uphold the fundamental rights and freedom of data subjects set out in the Act as discussed above. Where the data controllers and or data processors fail in their responsibility the breach of data subject's right will occur and if this happens the data subject will be entitled to certain remedies.

If a data subject feels that any of his rights has been violated, or he is aggrieved by the decision, action or inaction of a data controller or data processor in violation of his right or the Act, he has the right to make a complaint to the Data Protection Commission [33]. The commission may investigate the data subject's complaint if it does not appear frivolous or vexatious [34]. In doing so, the commission may make representation to the data controller or data processor on behalf of the data subject (the complainant) [35].

From the investigation, if the Commission is satisfied that a data breach has occurred, it shall issue a compliance Order in writing specifying the provision of the Act that has been breached by the data controller or data processor [36]. The compliance Order is also required to state the specific measures to be taken by the data controller or data processor to remedy the breach and avoid subsequent breaches and the time frame for implementing such measures. It is further required by the Act to state that the data controller or data processor has the right to judicial review of the Order within 30 days of the making of the Order [37].

The Compliance Order may include a warning order; an order requiring the data controller or data processor to comply with the provision of the Act; an order requiring the data controller or data processor to comply with the request of the data subject in the exercise of his rights under the

Act; an order requiring the data controller or data processor to cease and desist from such data-breaching acts [38].

Notwithstanding the complaint to the commission and the administrative remedies available, a data subject who suffers injury, loss or harm as a result of the violation of the Act or breach of his rights by a data controller or data processor, may also recover damages against such data controller or data processor in civil proceedings [39]. By the provision of section 51 of the Act, it is clear that for the data subject of be entitled to damages, he must have suffered injury or damage as a result of the breach. This is in line with the decision of the CJEU in *UI v Österreichische Post AG* [40].

Data security and measures to safeguard the rights of data subjects

The Act obliged the data controllers and data processors to implement appropriate technical and organizational measures to safeguard and ensure the security, integrity and confidentiality the rights of data subjects in their possession or control [41]. Where the data controller and or data processor fail to live up to this responsibility, he may be liable in damages to the data subject for any breach resulting there from. The data controller and or data processor may also acquire other liabilities such as penalty, fine or account for profit from the breach.

There are certain measures and practices that data processing organisations and their data controllers and processors can adopt to safeguard the fundamental rights of data subjects enshrined in the Act, thereby discharging their statutory obligations.

Some of the technical and organizational measures and practices that can be deployed to safeguard the rights of data subjects are:

1. **The adoption of strong data protection/privacy polices:** if a strong data privacy policy is made by an organization, reviewed regularly, and implemented vigorously, it will enhance compliance with the Act. Data controllers have a legal duty to display in a simple and conspicuous manner a privacy policy in any means through which personal data is being collected or processed [42]. The privacy policy is required to state amongst others, the issue of consent, description of data to be collected, purpose and method of collection and data processing principles. This will provide certain information to the data subject thereby satisfy the data controller's obligation to provide the data subject with information.

2. **Deployment of data and system protecting software:** this practice has to do with the use of strong anti-virus to protect systems and devices where personal data are processed, stored and retrieved. The organisations need to make it a practice to update such software and antivirus intermittently to ensure their effective protection.

3. **Adoption of data encryption practice:** the Act listed encryption of personal data as one of the measures to be implemented by the data controller and data processor [43]. This is a security method where information is encoded and can only be access or decrypted by a user with the correct encryption key [44]. Here, an algorithm is used in preventing unauthorized access to data. An encrypted data can only be accessed by using the right encryption key. This therefore means that if data theft occurs in respect of encrypted data, the stolen data would not be useful to the thief as he cannot access same without the right encryption key.

4. **Keeping and periodic review of data inventory:** a data inventory is a complete record of the information resources kept up by the data controller or its organisation [45]. This is important for an organisation to gain an understanding of data that it stores, identify a risk and mitigate the risk in order to comply with data protection laws. The practice of periodic review of data inventory by an organisation would enable the data controller to know what data and how much of the data that it has collected, processed and stored. This will enable the data controller to promptly identify and delete or erase personal data for which the purpose of processing has been achieved, thereby fulfilling its statutory obligation. Conducting a periodic data inventory or information stock decreases liability by enabling an agenda for security and improves the capacity to assign responsibility for the nature of the information gathered and processed.

5. **Periodic assessment of risks to processing systems:** data controllers and data possessors should regularly assess the risks and services, including where the processing involves the transmission of data over an electronic communications network' [46]. The systems and devices used in processing, transmission, storage and retrieval of persona data should be subjected to frequent examination to enable the discovery of any risk that may lead to data breaches.

6. **Minimal data collection:** this practice entails that the organisation processes personal data only necessary for the specific purpose of processing. Where a particular data is not needed by the organisation such data should not be collected or processed. The less data collected the less liability accrues. That is, the more quanta of data, the higher the organisation would be exposed to liability for breach of rights of data subjects.

7. **Procurement of voluntary consent from data subjects prior to processing:** every data processing organisation should ensure that it procure voluntary consent from data subjects before proceeding to collect, process, store and retrieving data of data subjects. This will greatly reduce data breach liability.

8. **Periodic assessment and evaluation of all measures:** this involves the periodic assessment and evaluation of the effectiveness of all measures put in places in view of the present and evolving risk and the regular updating of the measures. This will enable the introduction of new measures to make up for any inadequacy in the existing measures and cater for novel risks.

Conclusion and Recommendations

The Act has established comprehensive rights of data subjects and detailed procedure on how the data subject can obtain redress including damages, where breaches occur. What is left is the implementation of these soaring provisions. Consequently, we recommend a comprehensive and diligent implementation with the ultimate goal of achieving data security and safeguarding the fundamental rights of data subjects as set out in the Act. The Data Protection Commission should, without any delay, swing into action by setting out all necessary guidelines, regulations and practical measures geared toward effective implementation and enforcement of these laudable rights of data subjects.

Data controllers and processors should establish adequate data security measures to ensure that the rights of data subjects are preserved and not infringed upon. They can do this by implementing the measures identified and discussed above. All data processing organizations should train and retrain their data controllers and data processors on the rights of data subjects and their responsibilities under the Act.

References

1. This Regulation was issued by the National Information Technology Development Agency pursuant to section 6 of the National Information and Technology Development Agency (NITDA) Act 2007.
2. Nigeria Data Protection Act 2023, section 65.
3. Nigeria Data Protection Act 2023.
4. Ibid, section 65.
5. Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 1.3 (xiv).
6. See Article 1,African Union Convention on Cyber Security and Data Protection (2014).
7. Nigeria Data Protection Act 2023.
8. Ibid, section 24(2).
9. Ibid, section 24(3).
10. Ibid, section 24(1)(a).
11. Ibid, section 25(1)(a).
12. Ibid, section 25 (1)(b).
13. Ibid, section 25(2).
14. Ibid, section 24(1) (b).
15. Ibid, section 24(1) (c).
16. Ibid, section 24(1).
17. Ibid, section 34(1).
18. Ibid, section 35(1).
19. Ibid, section 36(1).
20. Ibid, section 38.
21. Ibid, section 37(1).
22. Ibid, section 34(1)(a)(vi).
23. Ibid, section 35(1).
24. Ibid, section 36(2).
25. Ibid, section 38(1).
26. Diker Vanberg, A. and Ünver, MB., 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' European Journal of Law and Technology, Vol 8, No 1, 2017.
27. Nigeria Data Protection Act 2023, section 37.
28. Roig, A., 'Safeguards for the right not to be subject to a decision based solely on automated processing (Article22 DPR)' European Journal of Law and Technology, Vol 8, No 3, 2017.
29. Nigeria Data Protection Act 2023, section 37(3).
30. Ibid, section 37(3).
31. Case C-154/21 Österreichische Post (the Österreichische Post case) delivered 12 January 2023, <https://www.dpocentre.com/cjeu-decision-data-subjects-have-the-right-to-know/> accessed 29 June 2023.
32. (C-487/21) ("CRIF") (4 May 2023)<https://www.whitecase.com/insight-alert/somewhere-between-a-summary-and-data-dump-cjeu-finds-controllers-must-provide-data> accessed 29 June 2023.
33. <https://curia.europa.eu/jcms/jcms/Jo2_7052/en/> accessed 29 June 2023 and
34. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-06/cp230107en.pd> accessed 29 June 2023.
35. In the case, an employee of bank Pankki S who was, at the same time, a customer of that bank, learnt that his
36. personal data had been consulted by other members of the bank's staff, on several occasions. He then asked Pankki S to inform him of the identity of the persons who had consulted his customer data, the exact dates of the consultations and the purposes for which those data had been processed. Pankki S refused to disclose the identity of the employees who had carried out the consultation operations on the data. The applicant applied to the Data Protection Supervisor's Office, Finland, seeking an order that Pankki S provide him with the information requested. The application was rejected, and the applicant maintained an action before the Administrative Court of Eastern Finland, which asked the Court of Justice of EU to interpret Article 15 of GDPR.
37. (C-300/21) (4 May 2023), <https://www.whitecase.com/insight-alert/civil-plaintiffs-must-prove-gdpr-damages-says-cjeu> accessed 29 June 2023. In the case, an individual sued Österreichische Post AG (Post AG), the Austrian postal service, seeking EUR 1,000 as compensation for non-material damage stemming from Post AG's allegedly unlawful processing of his personal data. The Post AG processed data from which it deduced Plaintiff's high affinity for a certain Austrian political party, without his consent. Although the information was not transmitted to third parties, Plaintiff claimed that the storage of data on his alleged political opinions temporarily caused him "great upset, a loss of confidence and a feeling of exposure."
38. Ibid, section 65.
39. Ibid, section 41(1).
40. Ibid, section 41(2).
41. Ibid, section 14(7)(a).
42. Ibid, section 47(3).
43. Ibid, section 47(3)(d) and section 50.
44. Ibid, section 47(2).
45. Ibid, section 51.
46. Österreichische Post AG case(n 43).
47. Nigeria Data Protection Act 2023, sections37(3) and 39(1).
48. NDPR2019 (n 6), Paragraph 2.5.
49. Data protection Act 2023,section 39(2)(b).
50. <https://www.forcepoint.com/cyber-edu/data-encryption>accessed29June 2023.
51. What is data inventory and why is it important? <https://satoricyber.com/data-management/what-is-a-data-inventory-and-why-is-it-important>accessed 29June 2023. Data Protection Act, section 39(2).