CONSUMER DATA RIGHTS IN NIGERIA: AN ANALYSIS OF THE ARAKA V. E-CART JUDGMENT

Introduction

The judgment in Araka v. E-Cart Internet Services & Anor (FHC/ABJ/CS/195/2024) represents a pivotal moment in Nigeria's data protection jurisprudence. This case decided under the Nigeria Data Protection Act (NDPA) 2023, provides critical insights into how Nigerian courts interpret and apply data privacy principles in the digital economy. The ruling offers valuable lessons for businesses operating in Nigeria about lawful data processing, third-party data disclosures, and consumer rights protection.

This article analyses the Araka judgment and discusses practical implications for organisations handling personal data in Nigeria. In light of this seminal case, we will explore the NDPA's foundational principles, the court's interpretation of lawful processing requirements, and best practices for compliance

Legislative Framework

The NDPA 2023 establishes a comprehensive legal framework for data protection in Nigeria, with several key objectives outlined in Section 1:

1. Safeguarding fundamental rights: Protecting data subjects' constitutional right to privacy under Section 37 of the 1999 Constitution (as amended).
2. Regulating data processing: Establishing clear rules for lawful processing of personal data.
3. Promoting security best practices: Encouraging organisational measures that protect data security and privacy.
4. Ensuring accountability: Mandating that processing occurs fairly, lawfully and transparently.
5. Establishing regulatory oversight: Creating the Nigeria Data Protection Commission (NDPC) as an independent supervisory authority.

The Act applies broadly under Section 2 to data controllers/processors domiciled or operating in Nigeria, processing occurring within Nigeria and processing of Nigerian data subjects' personal data, even by foreign entities.

Key Principles of Data Processing

Section 24 of the NDPA establishes fundamental principles that controllers and processors must adhere to:

1. Lawfulness, fairness and transparency: Processing must meet lawful bases and be conducted transparently
2. Purpose limitation: Data collected for specified purposes cannot be further processed incompatibly
3. Data minimisation: Only adequate, relevant and necessary data should be collected

4. Accuracy: Personal data must be accurate and kept up to date
5. Storage limitation: Data should not be retained longer than necessary
6. Integrity and confidentiality: Appropriate security measures must protect against breaches

Lawful Bases for Processing

Section 25 specifies six lawful bases for processing personal data:
1. Consent: Freely given, specific, informed and unambiguous (Section 26 elaborates on consent requirements)
2. Contract performance: Necessary for executing a contract with the data subject
3. Legal obligation: Required to comply with Nigerian law
4. Vital interests: Needed to protect someone's life
5. Public task: Carried out for official authority or public interest
6. Legitimate interests: For the controller's or third party's interests, provided they don't override the data subject's rights

For sensitive personal data (defined in Section 65 to include genetic/biometric data, health information, sex life, political/religious views etc.), Section 30 imposes stricter requirements, generally requiring explicit consent unless specific exceptions apply.

The Araka v. E-Cart Case

The plaintiff, Mr Chukwunweike Akosa Araka, was a customer of Jumia Food (operated by E-Cart Internet Services Nigeria Limited). Through this platform, he ordered food from Domino's Pizza (owned by Eat 'N' Go Limited).

Key Facts Established in Court:

1. Data Collection: Jumia Food collected Araka's personal data (name, phone number, address) during account creation and order placement.
2. Data Sharing: Jumia shared this data with Domino's Pizza for order fulfilment.
3. Secondary Use: Seven months after his last order, Domino's began sending Araka direct marketing SMS messages promoting its products.
4. Objection: Araka requested cessation of marketing and erasure of his data, but the messages continued.
5. Legal Action: Araka sued both companies for violating his data privacy rights.

Legal Basis of the Suit:

Araka's suit alleged violations of:
- Section 37 of the 1999 Constitution (Right to privacy).
- Sections 24-26 of the NDPA (Principles and lawful bases for processing).
- Section 29 of the NDPA (Controller-processor obligations).
- Section 34 of the NDPA (Right to erasure).
- Section 36 of the NDPA (Right to object).
- Section 124 of the Federal Competition and Consumer Protection Act (FCCPA) 2018 (Protection against unfair commercial practices).

Justice Emeka Nwite's judgment provided key interpretations of the NDPA. The court affirmed that E-Cart (Jumia) was the data controller and Eat 'N' Go (Domino's) was the processor. Data sharing for order fulfilment was deemed lawful under the contract performance basis (Section 25(1)(b)(i)). However, using the data for marketing exceeded the original purpose and lacked a lawful basis.

Applying Section 65 definitions, the court determined that:
- E-Cart collected and determined the purposes and means of processing customer data for food delivery services.
- Dominos processed this data solely for order fulfilment on behalf of E-Cart.

The court emphasised Section 24(1)(b), which requires that further processing must be compatible with the original purpose. It rejected Domino's legitimate interest argument (Section 25(2)), finding that marketing overrode Araka's rights. The court assessed compatibility under Section 24(4) and found that marketing was incompatible due to:
- Unrelated purposes: Delivery vs. promotional outreach.
- Privacy impact: Contact details were used in a way that adversely affected privacy expectations.
- Negative consequences: Unwanted intrusion and loss of control over personal data.
- Lack of safeguards: No additional protections were implemented.

The court also ruled that Araka had no reasonable expectation that his data would be used for marketing (Section 25(2)(c)). Furthermore, it clarified that opt-out mechanisms do not replace the need for initial consent (Section 26). There was no evidence that Araka had consented to the use of his data for marketing when providing his details for deliveries.

The court found that E-Cart fulfilled its controller obligations under Section 29 by:
- Disclosing data sharing in its privacy policy (Exhibit Ecart 1).
- Having an On-Demand Service Agreement with Domino's (Exhibit Ecart 3).
- Taking prompt action upon being notified of misuse (sending a letter demanding cessation).

However, the court reinforced that processors remain directly liable for NDPA violations. Dominos could not shift blame to E-Cart for its independent decision to use the data for marketing.

Court Orders and Remedies:

The court granted several declaratory reliefs and ordered:
- Immediate cessation of marketing messages.
- Erasure of Araka's personal data from Domino's systems.
- N3 million in general damages against Domino's, reduced from the N120 million initially claimed.

Significance of the Judgment:

This ruling strengthens consumer rights protections by:
- Upholding the right to object (Section 36), particularly in relation to direct marketing, which must stop immediately upon objection.
- Reinforcing the right to erasure (Section 34) when data is no longer necessary for its original purpose and lacks any lawful basis for retention.

- Clarifying the distinct liabilities of controllers and processors, ensuring that processors cannot misuse data under the guise of prior lawful sharing.
- Linking data protection with consumer protection laws, broadening enforcement mechanisms against data misuse.

The Araka case demonstrates Nigerian courts' willingness to enforce data protection rights. Organisations should also be aware of NDPC's enforcement powers to impose administrative fines. Section 48 establishes a tiered penalty system. For non-major controllers/processors, greater of ₦2 million or 2% of annual gross revenue and for major controllers/processors (defined in Section 65 as those processing data of significant numbers or sensitive categories), greater of ₦10 million or 2% of annual gross revenue. Also, Section 49 provides for fines and/or imprisonment up to one year for non-compliance with NDPC orders.

Practical Implications for Businesses

Compliance Recommendations for Data Controllers

1. Third-Party Vendor Management:

- Conduct thorough due diligence on processors
- Implement detailed written contracts specifying:
  - Processing purposes and limitations
  - Security requirements
  - Audit rights and compliance monitoring
  - Breach notification procedures
- Maintain records of processor agreements (Section 29(2))
-

2. Data Mapping and Purpose Specification:

- Document all processing activities and data flows
- Clearly define purposes for collection at the point of data gathering
- Assess compatibility before any new processing (Section 24(1)(b))

3. Consent Mechanisms:

- Implement granular consent for distinct processing purposes
- Avoid pre-ticked boxes or implied consent
- Provide easy withdrawal methods (Section 35)

4. Consumer Rights Processes:

- Establish procedures for handling:
  - Access requests (Section 34)
  - Erasure requests
  - Objections (especially for direct marketing)
- Train customer service teams on data subject rights

Compliance Recommendations for Data Processors

1. Processing Scope Adherence:

- Only process data for the controller's specified purposes
- Seek controller authorisation for any additional uses
- Implement internal controls to prevent function creep

2. Controller Communication:

- Promptly notify controllers of:
  - New sub-processors (Section 29(1)(e))
  - Data breaches (Section 40)
  - Compliance difficulties

Conclusion

The Araka v. E-Cart judgment reinforces commitment to robust data protection under the NDPA 2023. It establishes strict boundaries for data processing, emphasising purpose limitation and fresh consent for secondary uses. The ruling highlights direct processor liability and upholds enforceable consumer rights to object and erasure. Businesses must prioritise transparent data practices, granular consent, and vendor oversight to avoid penalties. This decision sets a clear precedent for future cases, signalling stronger enforcement of privacy rights. Ultimately, compliance is now critical for both legal adherence and consumer trust in Nigeria's digital economy.

Authors:

Confidence Amuda – Senior Consultant & Research Lead
Confidence is a privacy and information security professional that excels at advising compliance with global privacy laws, cybersecurity regulations, risk assessments and compliance audits. Confidence can be contacted at

E-mail: Confidence.amuda@privalexadvisory.com

Favour Awamakinde – Data Protection Trainee
Favour is a dedicated data protection trainee at PrivaLex with background in corporate and commercial legal practice. Favour manages clients' relations at PrivaLex. Favour can be contacted at

E-mail: Favour.awamakinde@privalexadvisory.com

Take Action Today!

At PrivaLex Advisory, we help Nigerian businesses understand and comply with the Nigeria Data Protection Act (NDPA) 2023—especially in light of landmark cases like Araka v. E-Cart Internet Services & Anor. This pivotal judgment offers real-world guidance on lawful data processing, third-party disclosures, and upholding consumer rights in Nigeria's digital economy.

We support small and medium-sized enterprises by interpreting legal obligations, developing privacy-first data practices, and building systems that align with the NDPA's key principles—from consent management to data minimisation and security safeguards.

UK Office: Suite 5058, Unit 3A, 34-35 Hatton Garden, Holborn, London ECIN 8DX

Nigerian Office: Block E, New Providence Garden, Opposite Russel International School, Lekki, Lagos.

Landline: +234 (0) 813 358 6403 -Nigeria
+44 (0) 3030401065 -London

Website: www.privalexadvisory.com

E-mail: contact@privalexadvisory.com