T & A
LEGAL

Key Lessons for E-Commerce Businesses from the Case of Chukwunweike Akosa Araka v. Ecart Internet Services Limited & Eat 'n' Go Limited

Authors

Gbemisola Mosuro
Partner

Sharon Okpo
Senior Counsel

Obinna Egwu
Associate

Introduction

The recent decision of the Federal High Court in Akosa v. **Ecart Internet Services Ltd** and anor. sets a major precedent on how the Nigeria Data Protection Act, 2023 (the "NDPA") is enforced, particularly against unsolicited direct marketing. It is an important case that tested the provisions of the NDPA and confirmed that individuals can efficiently hold businesses accountable for breaching their data privacy rights.

With this article, we aim to highlight the significance of this case to e-commerce businesses and other digital services providers. In the course of their interaction with customers' data it is important to pay attention to the lessons and sentiments of the court in the case. The judgment sends a clear message **that data privacy is a binding legal duty, not a matter of discretion.**

Facts of the Case

Chukwunweike Akosa Araka ("Araka") received an unsolicited promotional SMS from Eat n Go Ltd's Dominos Pizza ("Dominos"). He had never given his personal data directly to Dominos. Instead, he placed a food order using the now defunct Jumia Foods platform, owned by Ecart Internet Services ("Ecart"), which lists several food vendors on its platform for customers to pick from. Through its service partnership with Dominos, Ecart shared Araka's phone number to facilitate food order delivery when Araka placed orders. However, Dominos went further to use the data to send him direct marketing message, without first obtaining his explicit consent for such use of his personal data.

Following this, Araka formally sent a notice to Ecart withdrawing any consent for such messages and requested the deletion of his personal data. Ecart complied by relaying this deletion request to Dominos. Araka used another food delivery platform to order from Dominos, and Dominos, on the other hand, continued sending marketing content even after his withdrawal, demonstrating a failure to obtain due consent, respect the clear limits of data processing, right to be forgotten, right to withdraw consent to receive marketing contents, and consent as provided in sections 25 (1), 24 , 34 (1)(d), and 36(4)of the NDPA, 2023 respectively.

Araka proceeded to file a suit seeking ₦125,000,000.00 (One Hundred and Twenty-Five Million Naira only) in damages for the breach of his data privacy rights. He requested general, exemplary, and litigation cost damages.

Position of the Respondents

Ecart: Ecart, which happens to be the 1st respondent in this case, opined that it had implemented proper safeguards and clearly defined the purpose of sharing Araka's data with vendors, which was for facilitating the on-demand food delivery services. They further opined that any further use of the data shared with Dominos beyond the original scope and further use for marketing purposes was not at its instruction. In their defense, they further disclosed that on receiving the Claimant's first complaint of data breach, they promptly notified Dominos of Araka's deletion request, hence absolving themselves of any further liabilities.

Dominos: Dominos, the 2nd Respondent contended that Araka had consented to processing his data for marketing when he placed orders, and that even after receiving his initial data deletion request from Ecart, it continued to send any further messages when he resumed placing orders via another food delivery platform - Glovo. They further indicated that each marketing message came with an opt-out mechanism embedded in same to allow recipients to easily discontinue receipt of the direct marketing messages.

Judgment

On the liability of the Respondents, the Court held as follows:

Ecart: The Court agreed that Ecart's role was limited to what was necessary to fulfill its service. That is, order processing and delivery through its platform. It did not use the data for marketing and acted appropriately by forwarding Araka's complaint and deletion request to Dominos. Since it did not exceed the scope of its initial data use or ignore the complaint, the Court found no liability on its part.

Dominos: The Court held that Dominos used Araka's personal data for direct marketing without first securing his clear consent. It did not matter that their messages included an opt-out feature. The real issue was that Araka's consent was not obtained first and that there was no lawful bases for sending the messages in the first place. Furthermore, after Araka objected to receiving the marketing messages, delivery of same continued. This was a clear violation of both his rights under the NDPA and his constitutional right to privacy. As a result, the Court ordered Dominos to stop all direct marketing to Araka, erase his personal data, and awarded him ₦3,000,000.00 (Three Million Naira only) in damages.

Significance of Araka's Case

From the case, one key issue raised is the legal effect of a data subject's withdrawal of consent, but even more importantly, what happens when no consent was given in the first place.

Under Section 25 of the NDPA, consent is one of the lawful bases which must be considered before processing any individual's personal data. According to the NDPA, the data subject must have given and not withdrawn consent for the specified purpose or purposes for which personal data is to be processed. While the court did not consider the provisions of the NDPC General Application and Implementation Directive (GAID) 2025 in its decision as it was not yet in force, Article 18 of the NDPC GAID provides that consent is the only lawful bases for processing personal data in relation to any direct marketing activity. It is therefore a fundamental and foundational requirement that before a business can send marketing contents to a data subject, it must first obtain the subject's clear, specific and informed consent. Flowing from this obligation, Section 36(4) of the NDPA, goes on to provide for the additional right of a customer to object or withdraw consent to direct marketing at any time and the business must honour same.

While Dominos had a function in place which gave Araka the option to opt out of receiving direct marketing messages, the fundamental problem as the court had pointed out was that Dominos did not obtain Araka's consent to provide marketing messages in the first place. Hence, if there was no consent, then there was nothing to withdraw through the opt-out function.

This makes it clear that consent is a foundational requirement for the processing of personal data for direct marketing purposes. Businesses cannot rely on any other lawful bases to send direct marketing messages to customers except they obtain explicit consent from the individual customers.

The case also highlights breaches of the principles of purpose limitation principles under Section 24(1)(b) of the NDPA, 2023. Araka's personal data, collected solely to deliver his food order, was later used for a different purpose (unsolicited marketing) without his consent. This violates the requirement that personal data must be used strictly for the purpose for which it was collected. It is a common misconception and reflects poor data privacy culture when businesses assume that obtaining data for one purpose opens the door to broader use and the NDPA firmly and clearly shuts that door.

Each new purpose requires fresh, direct, and explicit consent save where same falls under the exceptions provided under the NDPA.

Key Lessons for E-Commerce Businesses from the Case

Develop a Robust Data Protection Policy and Internal Risk Framework: E-commerce platforms must put in place an internal structure that shows a commitment to data protection. This means having an internal data protection framework and documentation tailored to their operations. Such documentation should make provisions on how to receive and escalate privacy complaints, manage data breaches, and track privacy-related activities. Staff must also receive regular training to keep them up to speed with current data protection requirements and obligations under the NDPA and global data privacy/protection standards.

Collect Consent: In addition to processing personal data for direct marketing purposes, under the NDPA, there are other specific processing activities that also require consent mandatorily, like processing sensitive data, processing the data of a child, transfer of personal data outside Nigeria, etc. For these processing activities, businesses must make sure to collect clear, informed, and freely given consent from customers before processing their personal data. It is important that businesses carefully identify the purpose of processing to determine if they are mandatorily required to obtain consent, or if they can rely on other lawful bases to process such personal data.

Consent sought and obtained must be linked strictly to the specific purpose for which it was requested. For instance, if consent is given to process data for order fulfilment, businesses cannot use that same data for marketing or any other purpose without collecting fresh consent. Summarily, consent cannot be vague or blanket consents; it must be clear, specific and purpose-driven.

Know your processing activities, know your lawful bases, and ensure that the data subject is duly informed in your privacy policy or consent request document as well.

Maintain Proper Records of Consent, Communications, and Opt-Outs: There must be a system in place to document receipt of consent, withdrawal of the same, and communications regarding grant or retraction of consent. This is not optional. Good recordkeeping protects a business when legal questions as to compliance or disputes arise. It is equally relevant in assessing the strength and gaps of the data privacy/protection culture in a business.

Have Robust Contracts that Define and Limit Data Use: When partnering with third parties who may access customers' data as processors, contracts must clearly state the purpose for which the data is being shared and restrict any other use. For example, if customer details are to be exchanged with a third party for delivery, the agreement should expressly limit the use to just delivery and no marketing, profiling, or reuse, unless fresh consent is obtained by such third party. Strong contracts are the first line of defense in a data privacy claim, especially when they are backed up by strong indemnities for violation.

Ensure Transparency through a Clear and Accessible Privacy Policy: Every e-commerce platform should have a detailed privacy policy. This policy must state the identity of the data controller, the purpose of data collection, the legal bases for processing, how long data will be kept, and how the rights of the data subject will be protected. It should also clearly provide an avenue for the data subjects to make complaints.

Make Opting-Out Easy: Businesses should make it easy for users to give and withdraw consent, like clicking a box, replying "STOP," or switching off marketing preferences from a dashboard. Automation helps avoid mistakes and ensures compliance. The process for withdrawal of consent should not be long and cumbersome such as to deter a data subject from initiating or completing the withdrawal of consent.

Prepare for Breaches and Enforcement: There are real and stringent consequences for non-compliance with the NDPA. In consideration of the provisions of the NDPA on breaches, every business must have a damage control plan in case of a breach. Preparation makes all the difference when things go wrong. Breaches are hardly ever expected, even with the best data protection practices deployed same can still happen. This is the reason preparation makes all the difference; it helps businesses manage such incidents better and quickly reduce damage and downtimes for the business, protects the businesses reputation, and when the plan is best aligned with the provisions of the NDPA on breach response, the business will be compliant with the law. Preparation also helps businesses identify and fix loopholes early, avoid panic, reduce losses, and bounce back faster when breaches occur.

Implement Regular Audits and Privacy Assessments: Businesses must continue to carry out internal audits from time to time to check if their data protection systems and framework are still relevant and in alignment with changing technology, services, or laws on data privacy/protection. Where activities involve a high risk to data subjects (e.g., large-scale marketing or profiling), a Data Protection Impact Assessment (DPIA) must be carried out.

Assign a Dedicated Data Protection Officer (DPO): If an e-commerce business processes a lot of personal data or runs operations of national relevance, the NDPA requires that businesses appoint a DPO. The DPO's role is to guide internal compliance, receive complaints, manage DPIAs, and act as the business's point of contact with NDPC.

Conclusion

The outcome of Araka's case is very relevant to the e-commerce industry. Even though Nigeria is not yet a highly litigious jurisdiction on the subject, businesses must acknowledge that consumers and data subjects are becoming increasingly aware of their data rights. E-commerce players, especially those who rely heavily on customer data for insights and targeted service delivery, must understand that data is a business asset that comes with legal and ethical responsibilities which must be complied with.
Ultimately, e-commerce providers must treat the case precedent as an opportunity to examine their business processes and data privacy/protection culture against the global best data protection practices and apply all relevant data protection laws towards safeguarding consumer trust, avoiding crippling fines and reputational damages.

T & A LEGAL

If you require any further information or professional advice on the Data Privacy & Protection, you can reach out to our Data Protection Desk at *contactus@tundeadisa.com* and we will be happy to provide any assistance you may need.