THE CONSENT CONUNDRUM IN DATA PROTECTION COMPLIANCE: A REVIEW OF MOLEHIN V. UBA

abcs Alert

Volume 2 October 2025

In today's digital economy, personal data is often described as the new oil. Financial service providers thrive on collecting, storing, and processing personal information to advance their operations. However, the monetisation of data has simultaneously heightened the risk of misuse, unauthorised processing, and outright abuse of individuals' rights.

Against this backdrop, the Federal High Court in Miss Molehin Folashade v. United Bank for Africa PLC examined the relationship between the constitutional right to privacy, guaranteed under Section 37 of the Nigeria Constitution (CFRN), and the right to data privacy under the Nigerian Data Protection Regulation (NDPR) 2019, now replaced by the Nigeria Data Protection Act (NDPA) 2023 and the General Application and Implementation Directive (GAID). The central issue in the case was whether a bank could open and operate an account for a customer without her knowledge or consent. This decision will be reviewed through the prism of the NDPA and GAID, although the decision was reached on the basis of the NDPR.

Understanding the Background of the Case

In the above case, the Applicant, a remote employee of Eraconneckt (a US-based company), provided her UBA savings account details to her employer for salary payments. The employer remitted funds through an international money transfer platform into the account provided. However, instead of crediting the funds into the Applicant's existing savings account, UBA opened a new domiciliary account in her name, deposited the funds there, and notified her via SMS.

Upon notification of the credit, the Applicant contacted UBA to inquire why a new account had been opened without her directive or consent and requested closure of the account. The Bank refused. This led her to file a Fundamental Rights Enforcement (FREP) action, seeking damages, declarations that her right to privacy had been violated and an order of the court mandating UBA to close the domiciliary account.

UBA, in its defence, challenged the court's jurisdiction, arguing that the matter amounted to breach of a fiduciary duty, not a constitutional right. It further contended that at the time, Nigerian banking regulations prohibited foreign currency transfers into Naira accounts, and that the domiciliary account was opened in Miss Molehin's interest to avoid loss of funds.

Reviewing the Court's Findings

The Federal High Court held that UBA's actions violated the Applicant's constitutional right to privacy under Section 37 of the CFRN. By processing her personal data without her consent, the Bank acted negligently and unlawfully. The court granted declaratory reliefs that the conduct of the Bank violated the Applicant's right to privacy and the NDPR, and awarded damages to the tune of N 7,500,000, (Seven Million, Five Hundred Thousand) affirming that the right to privacy extends to the protection of personal data. In arriving at this decision, the Court considered the following critical factors:

Data Privacy as a Fundamental Right

In rejecting UBA's objection on jurisdiction where UBA contended that the suit of Miss Molehin falls within the domain of fiduciary duty breach, the Court held that violations of data rights under the NDPR (now NDPA) amount to violations of the right to privacy under the Constitution. Relying on Articles 1.1 and 2.9 of the NDPR, the court reasoned that Section 37 of the Constitution guarantee of privacy also encompasses protection of personal data and its lawful use.

Section 1(a) of the NDPA further cements this, stating that its objective is to safeguard the fundamental rights and freedoms of data subjects as guaranteed under the Constitution. Accordingly, unauthorised data processing is both a statutory violation and a constitutional infringement. Extant laws which protect right to privacy such as the NDPA are extensions of Section 37 of CFRN and a violation may give rise to fundamental rights actions provided such law is not inconsistent with the provisions of the Constitution.

Consent as the Cornerstone of Data Processing

In Molehin's Case, the Court emphasised that consent is central to lawful data processing. Under the NDPA, data processing is broadly defined to

include any operation performed on personal data, whether automated or manual. This encompasses collection, recording, storage, alteration, disclosure, and even deletion of personal data. Section 24 of the NDPA sets out the foundational principles of data processing. It requires that personal data must be:

1. processed fairly, lawfully, and transparently;
2. collected for specified, explicit, and legitimate purposes, and not further processed in a way incompatible with those purposes;
3. adequate, relevant, and limited to what is necessary for its purpose;
4. retained only as long as necessary;
5. accurate and up to date; and
6. Secured against unauthorised processing, access, loss, or destruction.

To process the data of a person, a data controller must have a lawful basis, with consent forming a primary basis. Section 25(1) (a) NDPA reinforces this by stating that processing is lawful where the data subject "has given and not withdrawn consent for the specific purpose." Article 17(9) GAID further requires controllers to provide data subjects with a clear and explicit choice to accept or decline consent. Section 26 NDPA also places the burden on the controller to prove or demonstrate consent was freely given, making it clear that silence or inactivity does not amount to or be taken as evidence of consent.

Thus, in Molehin's Case, the initial consent provided to the Bank by Miss Molehin was given only for the opening of a savings account, while her consent was not sought for the subsequent opening of the domiciliary account, albeit it was alleged to have been an action in her own interest by the Bank.

It is clear from the court decision that repurposing her data for opening for a domiciliary account without fresh consent was unlawful and incompatible with the original purpose for which the personal data was thus given. The Bank was unable to establish that consent was given for the opening of the domiciliary account. In addition, the refusal to close the unsolicited account compounded the violation, justifying the degree of damages awarded by the Court.

The Need for Alternative Lawful Bases for Data Processing

Although consent is one of the primary bases for lawful data processing, Section 25(1)(b) NDPA recognises other lawful bases as well: compliance with legal obligations, protection of vital interests, performance of public interest tasks, or pursuit of legitimate interests by the controller. These bases apply only in exceptional circumstances, such as emergencies where consent cannot reasonably be obtained.

Although UBA attempted to justify its conduct on the basis of customer's interest, citing restrictions on foreign currency transfers into Naira accounts, the Court rejected this defence because the Bank failed to demonstrate that it sought and obtained consent. There is no alternative lawful basis that justifies the processing of Miss Molehin's data towards opening a domiciliary account. Considering the peculiar facts of the case, what is clear is that consent was the only ground the Bank could have relied on to process the personal data of Miss Molehin for opening the additional account. Furthermore, the continued operation of the unsolicited domiciliary account undermined the Bank's claim of acting in her interest.

The Impact of the Decision on Data Processing in Nigeria

The judgment underscores that administrative convenience or internal banking rules cannot justify

supersede customer privacy rights or excuse unauthorised data processing. Any processing without consent constitutes both a statutory and constitutional violation.

Importantly, the case reinforces consent as the bedrock of Nigeria's data protection jurisprudence. It has also established a judicial precedent in data protection in Nigeria, raising public awareness of the need for data subject consent by organizations among Nigerians many of whom remain unaware of their constitutional rights to privacy, a violation of which can be the subject of a fundamental rights action in court. For data controllers, especially financial institutions, the decision is a cautionary tale: unauthorised processing carries liability not only in regulatory terms but also in civil litigation and hefty court awards and damages.

Enforcement and Remedies for Consent Violation

The NDPA provides multiple avenues for redress for violation of data subject privacy rights. Under Section 46, aggrieved data subjects may lodge complaints with the Nigeria Data Protection Commission (NDPC). Section 51 further entitles victims to damages in civil proceedings.

In Molehin v. UBA, the aggrieved bank customer took the route of civil litigation, filing a fundamental rights action for the enforcement of the Applicant's rights to privacy and the Court after making a positive finding, awarded damages and injunctive reliefs, affirming that non-compliance has tangible consequences. Beyond FREP action, data subjects may also:

1. Lodge complaints with the NDPC,
2. Lodge complaints with the data controller via the SNAG Template in schedule 9 of the GAID
3. Explore alternative dispute resolution (ADR), or
4. Sue in court for violation of data rights, contract, fiduciary duty, negligence, or other applicable causes of action.

The available remedies range from declarations and damages to injunctions, rectification, and damages. Where remedial steps are possible, an action for enforcement sets the wheel of remedy in motion;

Conclusion

Molehin v. UBA is a landmark case placing consent at the centre of Nigeria's data protection compliance framework. It reaffirms that personal data belongs to the individual, and any processing without consent is both unconstitutional and unlawful. The decision makes room for inference that remedial steps taken after a violation cannot substitute for the initial duty to obtain consent, though prompt corrective action may mitigate liability. For controllers, the lesson is clear: respect for data subjects' rights must guide processing decisions. For individuals, the case confirms that "my data, my right" is not merely aspirational but a legally enforceable reality in Nigeria.

5 /7 Ademola Street,
off Awolowo Road
South West Ikoyi, Lagos, Nigeria

19 Kolda Street,
Off Adetokunbo Ademola Crescent
Wuse II, Abuja, Nigeria

(+234) 906 902 2222
(+234) 906 903 3333
(+1) 917 809 4981
(+44) 203 807 9070

abcs-global.com
solutions@abcs-global.com