JACKSON, ETTI & EDU

DATA PRIVACY BREACHES IN NIGERIA'S FINANCIAL SERVICES SECTOR: A COMPLIANCE GUIDE FOR BANKS & FINTECHS

www.jee.africa

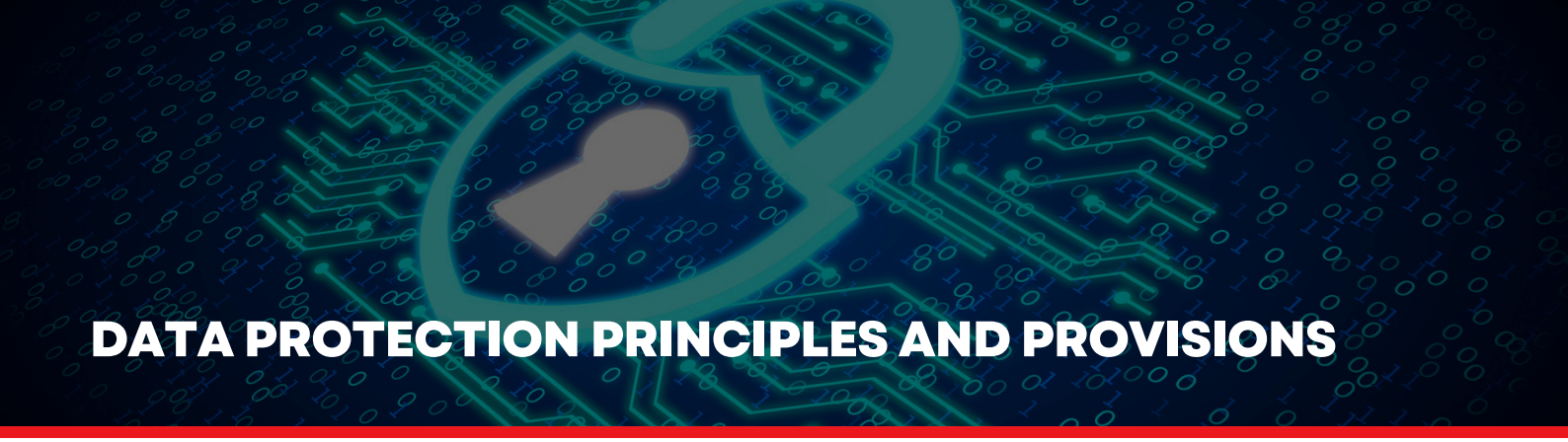
INTRODUCTION

The Nigeria Data Protection Commission (NDPC) serves as the primary authority for regulating data privacy in Nigeria. Together with the courts and other law enforcement agencies, the NDPC has consistently enforced compliance with the country's data protection laws – the Nigeria Data Protection Regulation (NDPR) and the Nigeria Data Protection Act (NDPA). The NDPC has played a proactive role in establishing and monitoring data privacy standards, holding companies accountable for breaches, and applying sanctions when necessary. Its assertive stance underscores the significance of protecting personal data in Nigeria, especially as the digital economy expands and data processing becomes more integral to business operations.

Enforcement Measures of the NDPC

In recent years, the NDPC has intensified its regulatory efforts towards commercial banks and other financial institutions due to their extensive handling of sensitive customer data. The Nigerian Data Protection Bureau (NDPB), before the establishment of the NDPC, had flagged the financial sector as one of the most worrisome in terms of data privacy compliance. This concern has reflected in the NDPC's actions, with numerous banks being fined for non-compliance. By 2023, several banks had been investigated and fined for violations of data privacy. More recently, Fidelity Bank was fined for breaching data protection regulations in relation to opening a bank account without the consent of the data subject. The courts have also supported these enforcement efforts by fostering adherence to data protection regulations through its decisions, for example, UBA was ordered by a court to pay N8,000,000 in damages for infringing on a data subject's privacy rights.

This regulatory rigour is not entirely new. Before the establishment of the NDPC, the National Information Technology Development Agency (NITDA), which previously oversaw data privacy regulation, levied fines against companies like Electronic Settlement Limited and Soko Lending Company Ltd. for violations. This pattern of regulatory action reflects the evolving landscape of data privacy in Nigeria. Commercial banks and financial institutions must now contend with stricter enforcement and the potential for severe penalties if they fail to adhere to the legal requirements for the protection of personal data.



DATA PROTECTION PRINCIPLES AND PROVISIONS

The Nigeria Data Protection Regulation (NDPR) and the Nigeria Data Protection Act (NDPA) form the legal and regulatory framework for data protection in Nigeria. Both laws contain key provisions for commercial banks and finance companies (in their capacity as data controllers or data processors) to note in formulating their data protection policies and standard operating procedures as it relates to data collection and processing. Below are some of the noteworthy provisions:

1. Lawful Processing

Under the NDPA, the lawful basis for processing personal data includes:

- Consent of data subject,
- Performance of a contract with data subject or towards said performance,
- Performance of a legal obligation,
- Protection of the vital interest of data subject or another person,
- Performance of a task carried out in public interest or in exercise of a public mandate,
- Legitimate interests.

The above are the metrics for measuring the legitimacy or otherwise of data processing. These metrics are disjunctive and individually adequate to form the basis for data processing. The law also prohibits data processing where it conflicts with the fundamental rights, freedoms and interests of a data subject or where it is done in a way not envisaged by the data subject.

2. Consent of the Data Subject

Under both the NDPR and NDPA, consent is a fundamental legal basis for the lawful collection and processing of personal data. Consent must be provided for a specific, legitimate, and lawful purpose, which is clearly communicated by the organisation controlling how the personal data will be processed. Where consent is withdrawn by the data subject, the bank may not have a lawful basis for processing personal data.

The NDPA defines consent as any freely given, specific, informed, and unambiguous indication, whether written, oral or an affirmative action, of an individual's agreement to the processing of personal data relating to them. The NDPA further strengthens this concept by establishing a detailed framework that underscores the critical importance of obtaining valid consent from data subjects.

In the Fidelity Bank scenario mentioned above, although internal investigations revealed that the account in question was never operational due to incomplete documentation, this defence does not address the primary issue of whether the bank was entitled to process the complainant's data in the first instance.

This is premised on the provision of the NDPA that mandates data processors and controllers to inform data subjects before processing their data. Moreover, under the NDPA, the data controller (in this case, Fidelity Bank) has the burden of proving that it obtained the data subject's' consent before processing their data.

3. Rights of a Data Subject

The law provides for the rights of data subjects as it relates to the processing of their data. They include:

- The right to lodge a complaint with the NDPC;
- The right to be informed about how personal data is used;
- The right to access personal data;
- The right to have personal data erased in certain circumstances;
- The right to restrict processing of personal data in certain circumstances; and
- The right to object to processing of personal data in certain circumstances.

4. Obligations of Data Controllers/Processors

Data controllers and processors must adhere to the standards and obligations set forth in the NDPA and implement appropriate technical and organizational measures to maintain the security, integrity, and confidentiality of personal data. These obligations also extend to 3rd party data processors engaged by data controllers/processors. Data processors must also provide the data controller or the engaging data processor with all necessary information to demonstrate compliance with the NDPA. This implies that finance companies and their 3rd party service providers or vendors, are jointly responsible for complying with the standards and obligations in the NDPA.

To formalize these responsibilities and ensure compliance, the NDPA requires that a written agreement should be executed between the data controllers and data processors, or between data processors, as applicable. This agreement serves as a binding legal instrument to hold all parties accountable for upholding the obligations under the NDPA with respect to the protection of personal data.

5. Obligation to Notify the NDPC of Personal Data Breach

A Data Controller is obligated to notify the NDPC within 72 hours of becoming aware of a breach that is likely to result in a risk to individuals' rights and freedoms. This notification should, where possible, contain information on the breach, including the categories and approximate number of affected data subjects and personal data records. Also, if a personal data breach poses a high risk to the rights and freedoms of a data subject, the data controller must promptly notify the affected data subject in clear and plain language, providing advice on mitigating potential adverse effects.

6. Sanctions Against Defaulting Data Controllers/Processors

The NDPR provides the following penalties (in addition to any other criminal liability) for breaches of the rights of a data subject:

- In the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater.
- In the case of a Data Controller dealing with less than 10,000 Data subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million Naira, whichever is greater

The NDPA also imposes penalties based on the classification of the data controller or processor as follows:

- For data controllers or processors of major importance, the maximum penalty is the greater of ₦10,000,000 or 2% of the annual gross revenue from the preceding financial year.
- For those not classified as controllers or processors of major importance, the maximum penalty is the greater of ₦2,000,000 or 2% of their annual gross revenue from the preceding financial year.
- Imprisonment for a term not more than one year or both.

Other enforcement measures that could be adopted by the NDPC include the issuance of a formal warning about potential violations, issuance of an order mandating compliance with statutory provisions or data subject requests and issuance of a cease-and-desist order to stop unlawful activities. The NDPC may also require the data controller or processor to remedy the violation, compensate affected data subjects, account for profits from the violation, or pay a penalty or remedial fee.

In imposing sanctions, the NDPC will consider factors such as the nature and severity of the infringement, the purpose of processing, the number of affected data subjects, the level of harm and mitigation efforts, intent or negligence, cooperation with the NDPC, and the category of personal data involved.

7. Possible Defence of Corporate Bodies

The NDPA stipulates that when an offence is committed by a corporate entity or firm, the entity or firm and its principal officers are presumed culpable, unless the principal officers can demonstrate that the offence was committed without their consent, or connivance, and that they exercised all due diligence to prevent the commission of the same. This defence may absolve the bank or financial institution from any liability, subject to the discretion of the NDPC.

Relevance of Data Protection Compliance Organisations (DPCOs)

The NDPC is empowered to license Data Protection Compliance Organizations (DPCOs) to monitor, audit and report on compliance with the NDPA and other relevant regulations. DPCOs provide the necessary expertise, guidance, and support to organizations in navigating data protection laws effectively, thereby mitigating risks of non-compliance, avoiding penalties, and protecting an organization's reputation. They also play a critical role in enhancing an organization's data protection framework and ensuring that personal data is processed and handled in accordance with the law.

Jackson Etti & Edu is a Data Protection Compliance Organisation (DPCO) licensed by the NDPC. The Firm offers invaluable expertise, experience, guidance and support to numerous organisations to ensure compliance with Nigeria's data protection laws.

CONTRIBUTORS

Kodichinma Anigbogu
Senior Associate

Mercy Matthew
Associate

JACKSON, ETTI & EDU

Key Contacts

For further information, kindly reach the key contact below:

ITOHAN IRORO

Managing Associate,
Deputy Head of Intellectual Property Department.

E: itohan.iroro@jee.africa

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

Tel
+234-(02)-014626841/3,
+234-(02)-012806989

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.