Jackson, Etti & Edu

NITDA'S SANCTION OF ONLINE LENDING PLATFORM:

A Cautionary Tale For Fintechs

www.jee.africa

The National Information Technology Development Agency (NITDA), the governmental agency responsible for the growth and development of information technology in Nigeria which includes regulation of the use and protection of personal data in Nigeria has been at the forefront of data privacy and protection in Nigeria. NITDA since the release of the Nigeria Data Protection Regulation 2019 (NDPR) has continued to establish and enhance the framework for the use and protection of private data. In recent times, the agency has had course to exercise its powers by imposing sanctions on errant companies.

In the Fintech space, companies such as Electronic Settlement Ltd and recently Soko Lending Company Ltd have been penalized for non-compliance with the NDPR.
In the case of Soko Lending Company Ltd, creator of online loan product Sokoloan, NITDA in its press release indicated that the fintech company was sanctioned for the following infractions: -

1. Use of non-conforming privacy notice (contrary to Article 2.5 and 3.1(7) of the NDPR);
2. Insufficient lawful basis for processing personal data (contrary to Articles 2.2 and 2.3 of the NDPR);
3. Illegal data sharing without appropriate lawful basis (contrary to Article 2.2 of the NDPR);
4. Unwillingness to cooperate with the Data Protection Authority (contrary to Article 3.1 (1) of Data Protection Implementation Framework); and
5. Non-filing of NDPR Audit reports through a licensed Data Protection Compliance Organisation (DPCO) (contrary to Article 4.1(7) of the NDPR).

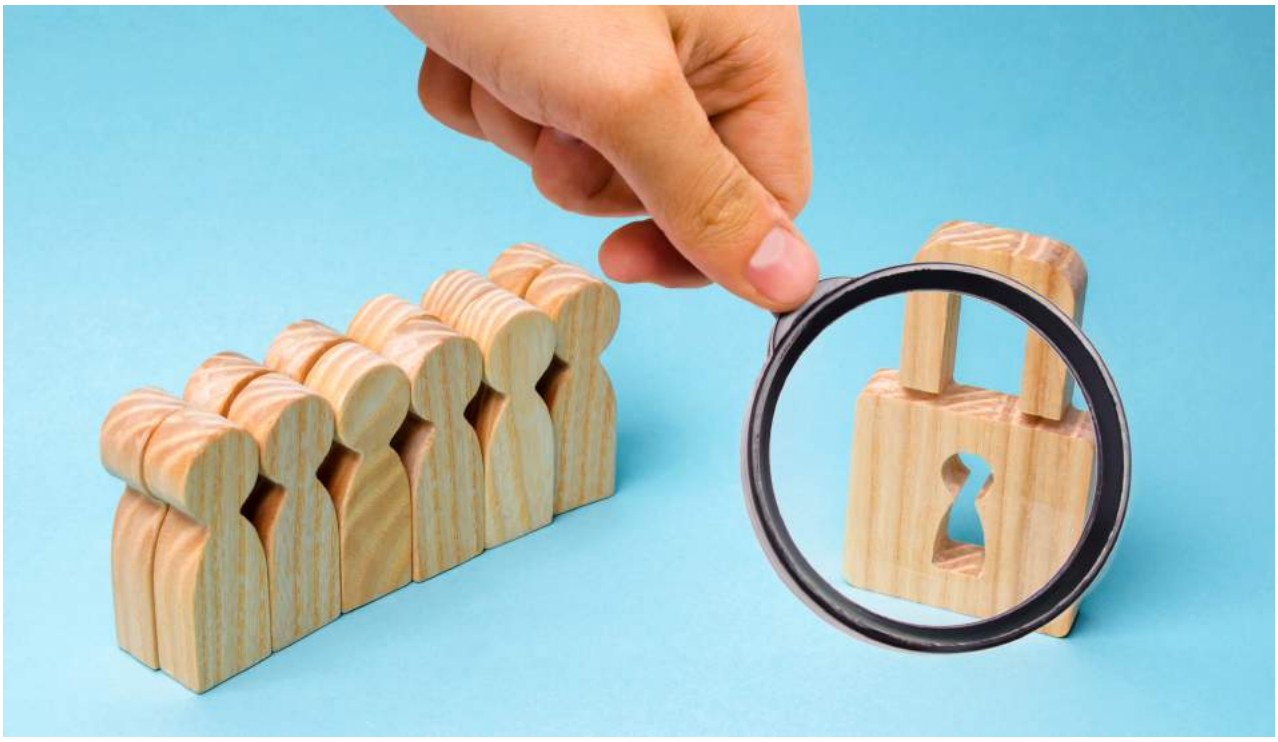
Each contravention will be treated below considering provisions of the NDPR and NDPR Implementation Framework ("the Regulations"):

Privacy Policy

The Regulations requires all organisations to publicly display its privacy policy in any medium for data collection. Such mediums include websites and mobile applications. A Fintech's privacy policy should cover the following points:

- Description of personal data and what is considered consent,
- Methods used to collect personal data
- contact information of the organisation, its DPO,
- purpose and legal basis for processing personal information
- the recipients of personal data and if there will be transfer of data abroad
- criteria for retaining data/retention period
- various rights of data subject: to withdraw consent, to request for personal data held to object to data processing, to lodge complaint etc.

Any failure to include the specifications required to be in the privacy policy may open up a Fintech to criminal and civil liabilities. The penalty for entities in breach of data subjects' privacy rights range from 1- 2% of their Annual Gross Revenue or 2 -10 million naira whichever is greater, in addition to criminal liability.



Lawful Basis

The Regulations permit the processing (any use) of personal data in either of the following five instances:

- with the consent of data subject,
- in performance of a contract with data subject or towards said performance,
- in performance of a legal obligation,
- where the vital interest of an individual requires it i.e., security or emergency situations or,
- further to a task in the public interest or in exercise of a public mandate

It has become common place for micro-loan Fintech companies to obtain access to phone contacts of the borrower. In the event that the borrower defaults, the lender may resort to contacting persons on the borrower's phone contacts list either in a bid to enjoin their assistance in recovering the loan or to embarrass the defaulter into paying up.

It must be pointed out that the borrower's consent to access phone contacts does not suffice as consent from the phone contacts themselves and thus there is no lawful basis for the lender to process the personal data of the phone contacts whether by reaching out or having the information stored in its systems.

This practice is also contrary to the data minimization principle. This principle requires an organisation to collect only personal data which it requires for its purpose e.g., providing the service. Where more data than necessary is obtained, the organisation is at a higher risk in the event of any data breach due to the increased volume of personal data that will be exposed.

Data Transfer

The Regulations provide that sharing of personal data with third parties is subject to several requirements:

- Presence of a written agreement between data controller and processor governing data processing activities.
- Information/awareness of data subject that personal data will be made available to third parties and for what purpose.

Where this is lacking and personal data is shared, such transfer of personal data would be termed illegal.

Companies that embed trackers in their applications that share customer data to third parties, are transferring personal data and must comply with the above.

Filing of Data Audit Report

The Regulations require Fintech companies that process personal data of over 2000 data subjects within 12 months to engage Data Protection Compliance Organisations (DPCO) who will conduct a data protection audit and file an audit report on behalf of the organisation.

An audit serves to assess the data protection compliance status for organisations and highlight areas of risks and processes that require improvement. Conducting data protection audits and filing reports is an annual exercise. The statutory deadline for the filing is the 15th of March each year. Fintech companies that fail to file their audit reports can be held liable for non-compliance with NITDA regulations, an offence under the NITDA establishment Act.

Startups with no operational history are apparently not within the ambit of the requirement to file an audit report. However, they are required to conduct a data protection impact assessment to identify and enable mitigation of data protection risks associated with the company's technology platform and business model. Fintech companies are encouraged to build and align their processes to incorporate data protection practices. This is referred to as data protection by design. By engaging a DPCO for advice on the appropriate data privacy requirements, Fintech companies can design their platforms and processes to ensure compliance with the NDPR and protection of their users' privacy rights.

Cooperation with the Data Protection Authority

The Regulations admits that NITDA requires the cooperation of all stakeholders, in furtherance of an effective compliance. This can be provided through stakeholder implementation of self-reporting mechanisms, notification to NITDA of existence of personal data breaches within specified period, obedience to administrative orders, and responding timeously to allegations of breach etc.

Where a Fintech company against whom complaints have been lodged fails to respond or expedite compliance with the NDPR, the entity will be considered to be uncooperative.

Conclusion

Data protection regulations and requirements have become a permanent feature of the regulatory framework for fintech companies.Beyond avoiding the regulator's bad books, complying with data protection laws ensure business processes are at par with global best practices and increases competitiveness and good standing on an international scale.

Proper data protection practices should be viewed as an investment that enables organisations to enhance internal processes, maximise efficiency in data processing, ensure proper management and itemisation of data, improve customer loyalty by ensuring privacy, and avoid privacy lawsuits.

Contributor
Kodichinma Anigbogu

Key Contacts

Jackson, Etti and Edu is a licensed Data Protection Compliance Organisation. For more information on how Fintech and other tech companies may comply with data protection law, please contact the Key Contacts below.

Adekunle Soyibo

Partner & Sector Co-Head, Financial Services

e: kunle.soyibo@jee.africa

Okey Nnebedum

Sector Co-Head, Financial Services

e: okey.nnebedum@jee.africa

Jackson, Etti & Edu

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

t: +234 (1) 4626841/3, (1) 2806989
e: jee@jee.africa

f: +234 (1) 2716889
www.jee.africa