KRISPY LEGAL
ATTORNEYS-AT-LAW



THIRD-PARTY ARTIFICIAL INTELLIGENCE AND DATA PROTECTION COMPLIANCE IN FINTECH: LEGAL OBLIGATIONS UNDER THE NIGERIAN DATA PROTECTION FRAMEWORK.

1. Introduction

The increasing adoption of Artificial Intelligence (AI) in the financial technology (fintech) sector has transformed how financial institutions assess creditworthiness, process loan applications, detect fraud, and make lending decisions. By analysing large volumes of personal and financial data, AI systems enable fintech companies to make faster and more efficient decisions. However, these benefits also introduce significant legal and ethical concerns, particularly where fintech companies rely on third-party AI vendors to process customers' personal data.

A fundamental question arises: can a fintech company escape responsibility for data protection violations simply because an external AI provider operates the technology? The answer is no. Outsourcing AI-driven processes does not eliminate a fintech company's obligations to protect personal data. Under Nigeria's data protection framework, organisations must ensure that personal data is processed lawfully, securely, transparently, and fairly, including where third-party service providers are involved.

This article examines the principal data protection obligations arising from the use of

third-party AI in fintech, with particular reference to the Nigeria Data Protection Act 2023 (NDPA) and the General Application and Implementation Directive (GAID) 2025.

2. The Legal Framework Governing Third-Party AI in Fintech

The principal legislation governing personal data protection in Nigeria is the Nigeria Data Protection Act 2023, which establishes the Nigeria Data Protection Commission (NDPC) and provides the legal framework for processing personal data. The Act is supplemented by the GAID 2025, which provides further guidance on implementing data protection obligations.

Under the NDPA, fintech companies must identify a lawful basis for processing personal data and comply with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and security. These principles apply whether processing is performed internally or through an external AI provider.

For instance, a fintech company that engages an AI vendor to evaluate loan applicants must ensure that the personal information supplied to the vendor is collected and processed lawfully and used only for legitimate, specified purposes. The commercial convenience of using AI does not justify indiscriminate data collection or processing.

3. Key Compliance Obligations

3.1. Privacy by Design and Data Protection Impact Assessments

Privacy by design requires fintech companies to incorporate data protection safeguards into the development, selection, and deployment of AI systems rather than treating privacy as an afterthought. These safeguards may include restricting access to personal data, anonymising information where appropriate, limiting data collection, and implementing effective security controls.

Section 28 of the NDPA requires a data controller to conduct a Data Protection Impact Assessment (DPIA) before processing where the nature, scope, context, and purpose of the processing are likely to result in a high risk to the rights and freedoms of data subjects. The GAID 2025 further addresses emerging technologies, including AI, and provides guidance on safeguards for their deployment.

A fintech company deploying third-party AI for credit scoring should therefore assess

potential risks before implementation. These may include inaccurate credit assessments, unauthorised disclosure of financial information, discriminatory outcomes, and decisions that adversely affect applicants' access to credit. The assessment should identify appropriate safeguards and document how the identified risks will be addressed.

3.2. Vendor Due Diligence and Data Processing Agreements

Engaging a third-party AI provider does not absolve a fintech company of its data protection responsibilities. Section 29 of the NDPA establishes obligations concerning the engagement and supervision of data processors, including appropriate security measures, assistance with data subjects' rights, and contractual safeguards.

Before engaging an AI vendor, a fintech company should conduct due diligence to evaluate the vendor's security practices, data handling procedures, technical competence, and capacity to comply with applicable data protection requirements.

The data processing agreement should clearly define the purposes of processing, the categories of data involved, confidentiality obligations, security standards, breach notification procedures, restrictions on further processing, and conditions for engaging additional processors. It should also address data retention and deletion when the contractual relationship ends.

These measures enable the fintech company to exercise meaningful oversight over the vendor and reduce the risk of unlawful processing, data breaches, and regulatory liability.

3.3. Pre-Deployment Testing and Continuous Monitoring

AI systems may produce inaccurate or harmful outcomes because of flawed algorithms, inadequate training data, or inappropriate assumptions embedded in their design. Deploying an AI model without sufficient testing may expose customers to unfair lending decisions and expose fintech companies to legal and reputational risks.

The GAID 2025 addresses safeguards for emerging technologies, including risk assessment, testing, evaluation of potentially discriminatory outcomes, and continuous monitoring. Fintech companies should therefore test AI systems before deployment to determine whether they process personal data appropriately, produce reliable results, and create disproportionate disadvantages for particular groups.

Testing should continue after deployment because changes in customer behaviour, data quality, or model performance may introduce new risks. Where testing reveals significant privacy or fairness concerns, the organisation should implement corrective measures, retest the system, or refrain from deploying it where the risks cannot be adequately mitigated.

3.4. Algorithmic Bias, Transparency, and Automated Decision-Making

Algorithmic bias is a significant concern in AI-driven lending. Models trained on historical financial data may reproduce existing patterns of discrimination. For example, an AI credit-scoring system may disadvantage applicants because of characteristics correlated with historical lending patterns, even where those applicants are otherwise creditworthy.

Fintech companies should periodically assess model outcomes, investigate unexplained disparities, and require vendors to provide sufficient information to evaluate the system's operation. Transparency is equally important. Customers should receive appropriate information about how their personal data is used and how AI influences decisions affecting them.

Section 37 of the NDPA provides protections concerning decisions based solely on automated processing that produce legal or similarly significant effects, subject to the applicable statutory conditions and exceptions. Fintech companies must therefore assess whether their automated lending systems fall within these provisions and implement the safeguards required by law, including appropriate opportunities for human intervention or review where applicable.

3.5. Data Security and Accountability

Fintech companies must implement appropriate technical and organisational measures to protect personal data against unauthorised access, disclosure, alteration, loss, or destruction. Such measures may include encryption, access controls, secure data transmission, staff training, vulnerability assessments, and incident response procedures.

Organisations should also establish clear internal responsibility for monitoring third-party AI systems and documenting compliance. Where an AI vendor experiences a data breach, the fintech company must assess its own obligations under the NDPA, including applicable breach notification requirements. Responsibility should not be

assumed to rest exclusively with the vendor.

4. Conclusion

The use of third-party AI in fintech presents significant opportunities to improve the speed and efficiency of credit assessment and lending. Nevertheless, these benefits must be balanced against the legal obligation to protect individuals' personal data and fundamental rights.

The NDPA 2023 and GAID 2025 establish a framework requiring fintech companies to approach AI adoption with accountability, transparency, and appropriate safeguards. Privacy by design, DPIAs, effective vendor agreements, pre-deployment testing, continuous monitoring, and periodic bias assessments are essential components of responsible AI governance.

Ultimately, outsourcing technology does not mean outsourcing accountability. Fintech companies must exercise meaningful oversight over third-party AI providers to ensure that innovation remains consistent with data protection law, fairness, and public trust. A sustainable digital financial sector depends not only on technological advancement but also on the effective protection of the people whose data makes that advancement possible.

References

1. Nigeria Data Protection Act 2023, particularly sections 28, 29 and 37.

2. Nigeria Data Protection Commission, “General Application and Implementation Directive (GAID) 2025”.

3. Nigeria Data Protection Act 2023: https://ndpc.gov.ng/ndp-act-2023/

4. Nigeria Data Protection Commission, General Application and Implementation Directive 2025: https://ndpc.gov.ng/wp-content/uploads/2025/03/NDP-ACT-GAID-2025-MARCH-20TH.pdf