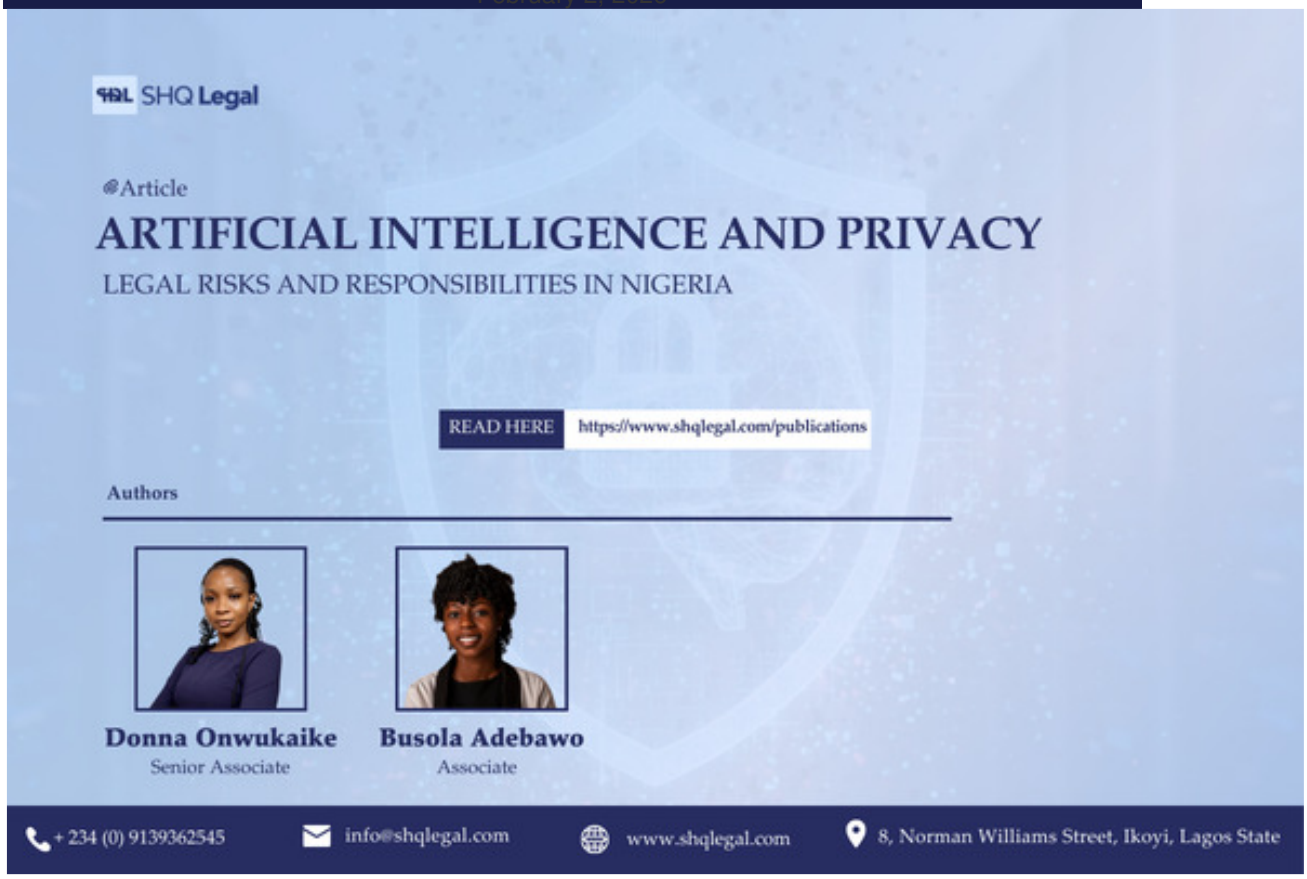
AI and Privacy in Nigeria: Legal Risks and Responsibilities Under NDPA 2023

February 2, 2026



ARTIFICIAL INTELLIGENCE AND PRIVACY: LEGAL RISKS AND RESPONSIBILITIES IN NIGERIA

Introduction

The increasing deployment of artificial intelligence across commercial, governmental, and social systems has reshaped how personal data is collected, processed, and utilised. Artificial intelligence ("AI") technologies, particularly those driven by large datasets, predictive analytics, and machine-learning models, enable organisations to derive insights about individuals at a scale and depth previously unattainable. While these capabilities support efficiency and innovation, they also raise significant questions for privacy law and data protection governance.

Traditional privacy frameworks were largely developed in response to earlier forms of data processing and may not fully account for the complexity, opacity, and speed of AI-driven decision-making. In practice, AI systems can process personal data in ways that challenge established legal principles, including meaningful consent, transparency, and accountability. Organisations deploying AI in Nigeria must navigate these complexities within the NDPA framework. The use of automated decision-making and profiling further heightens the risk of privacy intrusion, unfair outcomes, and discriminatory effects if not properly regulated.

Regulatory regimes across jurisdictions have begun to address these challenges by reinforcing foundational data protection principles such as data minimisation, purpose limitation, and individual rights in relation to automated processing. In Nigeria, the Nigeria Data Protection Act (NDPA), 2023 provides the legal framework for addressing privacy risks arising from emerging technologies, including AI. However, the rapid evolution of AI systems requires ongoing legal scrutiny to ensure that privacy protections remain effective and proportionate.

For organisations deploying or developing AI, understanding the legal risks and responsibilities associated with the processing of personal data is critical. Privacy compliance is no longer a secondary consideration, rather, it is a central legal and governance issue in the age of emerging technologies.

How AI is Transforming Privacy Law in Nigeria's Digital Era

Data protection and privacy laws have evolved considerably in response to changes in technology and society. Early legal conceptions of privacy were largely concerned with protecting individuals from physical intrusion, particularly within private spaces such as the home. As digital

technologies developed and personal information began to be generated, stored, and exchanged electronically in this 21st century, the focus of privacy protection gradually shifted from physical boundaries to the management and protection of personal data.

This shift gave rise to modern data protection regimes that regulate how personal information is collected, used, stored, and shared. Prominent regulatory frameworks in various jurisdictions reflect this evolution by imposing obligations on organisations to process personal data lawfully, transparently, and securely. The European Union's General Data Protection Regulation (GDPR), implemented in 2018, represents a significant milestone in this evolution, influencing laws in other jurisdictions.[1] Nigerian organisations increasingly look to GDPR as a benchmark for AI compliance best practices. These frameworks recognise that privacy in the digital age is closely tied to informational control and accountability, rather than physical seclusion alone.

However, the emergence of artificial intelligence has further tested the adequacy of existing privacy laws. Unlike conventional data processing methods, AI systems are capable of analysing large and diverse datasets to generate insights, predictions, and profiles about individuals. The ability of AI technologies to derive detailed personal insights without direct or explicit data disclosure has intensified global discussions about the limits of traditional privacy frameworks. These developments highlight the need for legal systems to continuously reassess whether existing principles and safeguards remain effective in addressing the unique risks posed by advanced data analytics and automated decision-making.

In Nigeria, this conversation is particularly relevant as organisations increasingly adopt data-driven technologies across multiple sectors. The challenge for regulators, businesses, and legal practitioners is to ensure that privacy laws continue to protect individual rights while allowing responsible innovation to flourish in an increasingly interconnected and automated digital environment.

Key Legal Risks in AI Processing of Personal Data Under NDPA

1. AI Transparency Requirements and Black Box Risks

Many AI systems operate as so-called "black boxes," making it difficult to explain how decisions are generated or how personal data influences outcomes. This creates practical challenges in

complying with core data protection principles such as transparency. Data protection laws generally require organisations to provide clear and meaningful information about how personal data is processed, including the logic and consequences of automated systems. In practice, this obligation is increasingly difficult to satisfy where machine-learning models are complex or continuously evolving. Globally, concerns have arisen around the use of **AI-driven facial recognition and surveillance technologies**, particularly in public security contexts, where individuals may be subject to continuous monitoring without a clear understanding of how their data is analysed or used.

This is illustrated in the prominent case of ***Glukhin v. Russia, decided by the European Court of Human Rights (ECtHR) in 2023***[2], where Russian authorities used facial recognition technology to identify Mr. Glukhin from images obtained from social media after he displayed a peaceful protest message in public. He was identified, tracked, and sanctioned without being informed that AI-driven facial recognition would be used or how the system operated.[3] The case challenged the lawfulness of using automated biometric surveillance without clear safeguards or transparency and examined for the first time, the legal risk associated with the use of facial recognition technology to identify an individual through images sourced from social media. The applicant was unaware that automated facial recognition would be used or how the system operated. The Court held that the use of AI-driven biometric surveillance without clear legal safeguards, transparency, or effective oversight amounted to an unlawful interference with the right to privacy. The absence of accessible information on how the technology functioned, how long data was retained, and how decisions could be challenged was central to the Court's reasoning. These developments illustrate the compliance risks organisations face when AI-driven processing lacks transparency or effective communication.

Failure to provide understandable explanations of AI-driven processing may expose organisations to regulatory scrutiny and undermine public trust.

2. Consent Requirements for AI Data Processing in Nigeria

Where organisations rely on consent as the lawful basis for AI-related data processing, such consent must be informed, specific, and freely given. This requirement is difficult to satisfy where individuals are unaware that AI systems are analysing their data or generating inferences about them.

Consumer-facing platforms, digital services, and public-sector systems often process large volumes of data through AI in ways that are not immediately apparent to users. Globally, concerns have been raised where biometric identification or profiling systems are introduced without meaningful user awareness or choice. This highlights the risk that consent obtained in AI contexts may be legally defective, particularly where individuals cannot reasonably understand the scope or consequences of the processing. Regulators have taken a strict approach to consent in AI-driven advertising and profiling.

In 2019, the French data protection authority (CNIL) fined Google €50 million after finding that users were not provided with clear, accessible information about how their personal data was used for personalised advertising.[4]Consent was obtained through pre-ticked options and bundled disclosures, which failed to meet the requirement for unambiguous, informed user action. Although Google relied on user agreement to terms and conditions, regulators found that users were not adequately informed about the scope of AI-driven profiling and advertising**.** The CNIL emphasised that the violations were ongoing rather than isolated, and that consent must be specific, actively given, and clearly separated from general terms and conditions. Google has repeatedly faced regulatory action in Europe over its use of personal data for targeted advertising.

Where individuals do not clearly understand how AI systems analyse and profile their data, consent may be legally defective, exposing organisations to sanctions and corrective orders.

3. Automated Decision-Making and Profiling

AI systems are data-driven by design. They often process personal data at scale, including behavioural data, location information, biometric identifiers, and inferred characteristics. In many cases, AI involves automated processing and profiling, which may have legal or similarly significant effects on individuals. AI-driven decisions, including credit assessments, recruitment screening, eligibility determinations, and behavioural profiling, may have legal or similarly significant effects on individuals and therefore raise heightened legal concerns. Data protection frameworks generally require additional safeguards where automated decision-making is used, including transparency, fairness, and, in some cases, human oversight.

Globally, financial institutions and employers have faced scrutiny over the use of automated systems that affect access to employment, credit, or essential services. In African and emerging markets, concerns have also emerged around the use of AI in social welfare administration and

identity management systems, where automated decisions may disproportionately affect vulnerable populations. In the landmark case of ***SCHUFA Holding AG (Case C-634/21, Court of Justice of the European Union (CJEU), 2023***[5]**,** the European Union Court of Justice of examined whether automated credit-scoring used by a private credit reference agency constituted prohibited automated decision-making. SCHUFA generated credit scores using algorithm mic profiling, which were relied upon by banks to determine whether individuals could obtain credit. The Court held that where an automated score plays a decisive role in decisions that significantly affect individuals, such processing may amount to unlawful automated decision-making if adequate safeguards, transparency, and the possibility of human review are absent.

For Nigerian organisations, understanding automated decision-making compliance is critical. The Nigeria Data Protection Act (NDPA) under section 37, also recognises the right of individuals not to be subject to decisions based solely on automated processing, including profiling, where such decisions produce legal or similarly significant effects, except in certain circumstances. The NDPA only permits automated decision-making where it is necessary for entering into or performing a contract, authorised by law, or based on the data subject's explicit consent. To use AI for automated decision making, the data controller must provide and implement appropriate measures to safeguard the fundamental rights and freedom of the data subject.[6]Such safeguards include transparency, the ability to contest the decision, and mechanisms for human review.

Thus, organisations must carefully assess whether human review mechanisms are required and whether individuals have effective means to challenge or seek review of AI-driven outcomes.

4. Bias and Discrimination

AI systems trained on biased, incomplete, or historically skewed datasets may produce discriminatory outcomes. This risk extends beyond data protection law and may implicate equality, human rights, and consumer protection principles. Experience from the deployment of AI systems demonstrates how AI-driven systems in areas such as financial services, recruitment, and law enforcement can reinforce existing social and economic inequalities. In this context, concerns have been raised about whether AI-based credit scoring or identity verification systems may unfairly disadvantage lower-income or marginalised groups. These issues underscore the importance of addressing bias at the design, training, and deployment stages of AI systems. From a legal perspective, discriminatory outcomes, whether intentional or not, can expose organisations to significant liability and reputational harm.

5. Cybersecurity Risks in AI Systems and Data Breach Prevention

The concentration of large volumes of personal data within AI systems significantly increases cybersecurity risk. AI platforms may create new vulnerabilities through data aggregation, model inversion, or unauthorised access to training datasets. A personal data breach involving AI-processed data can result in regulatory penalties, civil liability, operational disruption, and lasting reputational damage. Accordingly, organisations are expected to implement security measures proportionate to the risks associated with AI-driven processing, including continuous monitoring and regular risk assessments.

Legal Compliance Requirements for Organisations Deploying AI in Nigeria

1. Establishing Lawful Basis for AI Data Processing (NDPA Section 25)

Organisations deploying AI systems must identify and document a valid lawful basis for processing personal data. This obligation applies regardless of whether the processing is automated, outsourced, or embedded within third-party technologies. The lawful basis relied upon must be appropriate to the nature, scope, and impact of the AI processing activity.

In the AI context, this requires organisations to clearly define the purpose for which personal data is processed and to ensure that such purposes are specific, legitimate, and compatible with what has been disclosed to data subjects. **Section 25 of the NDPA** identifies the lawful basis upon which personal data may be processed, which are, namely consent, performance of a contract, compliance with a legal obligation, protection of vital interest, performance of a task carried out in the public interest, and legitimate interests, subject to appropriate safeguards. Where processing evolves over time, such as, where AI systems are retrained or repurposed, organisations must reassess whether the original lawful basis remains valid.

Reliance on consent, in particular, requires careful consideration. Consent must be informed, freely given, and capable of withdrawal, which can be difficult to guarantee in complex AI-driven

environments. Where alternative lawful bases are relied upon, organisations must ensure that the balancing of interests is properly documented and defensible.

2. Data Protection Impact Assessments (DPIAs) for AI Systems

Where AI-driven processing is likely to result in a high risk to the rights and freedoms of individuals, organisations are generally required to conduct a Data Protection Impact Assessment (DPIA) prior to deployment. This obligation is particularly relevant for AI systems involving large-scale processing, the use of sensitive or biometric data, or automated decision-making that produces legal or similarly significant effects.

DPIAs serve as a structured mechanism for identifying, assessing, and mitigating privacy risks at an early stage. They require organisations to evaluate the necessity and proportionality of the proposed processing, assess potential adverse impacts on data subjects, and document the technical and organisational measures implemented to address identified risks.

Under Article 7 of the General Application and Implementation Directive (GAID) 2025, data controllers and processors are required to conduct DPIAs in compliance with the Nigeria Data Protection Act where mandated by law or directed by the Nigeria Data Protection Commission. Article 28 of the GAID further requires a DPIA where data processing is likely to result in a high risk to the rights and freedoms of data subjects, having regard to the nature, scope, context, and purposes of the processing. This includes the introduction of new technologies, novel processing techniques, or large-scale data processing initiatives.

A DPIA is particularly required where:

a. the processing may result in unintended adverse consequences for the lives or livelihoods of data subjects.

b. such consequences pose risks to fundamental rights and freedoms, including the fundamental objectives and directive principles of state policy; or

c. the processing constitutes a limitation or derogation from the right to privacy guaranteed under Section 37 of the Constitution of the Federal Republic of Nigeria, 1999, ensuring compliance with the required provisions of the law.

The proper conduct and documentation of DPIAs plays a critical role in demonstrating accountability to regulators and may form part of an organisation's defence in the event of regulatory inquiries or enforcement action.

3. AI Transparency Obligations and Privacy Notice Requirements

Transparency is a cornerstone of lawful AI deployment. Organisations must ensure that individuals are clearly informed when AI systems are used to process their personal data and that such disclosures are made in a concise, intelligible, and accessible manner.

Privacy notices and related communications should explain:

i. that AI or automated processing is involved;

ii. the nature and purpose of the processing;

iii. the categories of data used; and

iv. the potential impact of such processing on individuals.

Where AI systems influence decisions that affect individuals, organisations should also explain the role of automation and any available avenues for review or objection. Effective communication not only supports legal compliance but also plays a central role in building trust and reducing reputational risk.

4. AI Governance Frameworks and Accountability Mechanisms

Effective AI compliance requires clear governance structures and accountability mechanisms. Organisations must ensure that responsibility for AI-related data protection obligations is clearly allocated, including oversight at senior management level. This includes maintaining proper documentation of AI systems, decision-making processes, and risk assessments, as well as implementing regular monitoring and review procedures. AI systems are not static; as models evolve, learn, or are updated, organisations must reassess their compliance posture to ensure continued alignment with legal and ethical standards. Where third-party vendors or AI service providers are involved, organisations must conduct appropriate due diligence and ensure that contractual arrangements clearly allocate responsibilities and safeguards.

5. Ethical AI Deployment and Building Stakeholder Trust

Beyond strict legal compliance, ethical considerations increasingly shape how AI technologies are regulated, adopted, and perceived. While legal and regulatory frameworks provide the formal rules governing the use of artificial intelligence, ethical considerations play an equally important role in shaping responsible data practices. The development and deployment of AI technologies raise complex questions that go beyond compliance, particularly in relation to individual autonomy, fairness, and trust. Public trust in emerging technologies depends not only on technical performance but also on fairness, accountability, and respect for individual autonomy.

Organisations that treat privacy as a core ethical value, rather than merely a regulatory obligation, are better positioned to sustain long-term innovation and public confidence. Ethical AI use closely aligns with legal principles: transparency supports informed consent, fairness mitigates the risk of discrimination, and accountability reinforces compliance and good governance.

Frequently Asked Questions on AI and Privacy in Nigeria

Q: What is NDPA Section 37 on automated decision-making?
A: NDPA Section 37 grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, where such decisions produce legal or similarly significant effects, except where necessary for contract performance, authorized by law, or based on explicit consent.

Q: When is a DPIA required for AI systems in Nigeria?
A: Under GAID Article 28, a DPIA is required where AI processing is likely to result in high risk to individuals' rights and freedoms, particularly for large-scale processing, sensitive data use, or automated decision-making with significant effects.

Q: What are the lawful bases for AI data processing under NDPA?
A: NDPA Section 25 identifies six lawful bases: consent, contract performance, legal obligation, vital interests protection, public interest tasks, and legitimate interests with appropriate safeguards.

Conclusion

Artificial intelligence presents significant opportunities for innovation, but it also amplifies privacy risks and legal responsibilities. Organisations that deploy AI must ensure that personal data is processed lawfully, transparently, and responsibly. Nigerian organisations must prioritize NDPA compliance as AI adoption accelerates across sectors. By embedding privacy into AI governance frameworks and prioritising accountability, organisations can reduce legal risk, build trust, and support sustainable innovation.

References

[1] Buang Jones Attorneys "The Evolution of Data Protection and Privacy Laws: A Comparative Analysis" https://buangjones.com/2023/07/20/evolution-of-data-protection-and-privacy-laws/#:~:text=Several%20landmark%20cases%20highlight%20the,particularly%20in%20social%20media%20companies. AccessedJanuary 22, 2025.

[2] Federal Bar Association "*Glukginv. Russia: The European Court of Human Rights' first step into the Age of AI Surveillance*" < https://www.fedbar.org/blog/glukhin-v-russia-the-european-court-of-human-rights-first-step-into-the-age-of-ai-surveillance/>accessed January 22nd, 2026.

[3] Federal Bar Association "*Glukginv. Russia: The European Court of Human Rights' first step into the Age of AI Surveillance*" < https://www.fedbar.org/blog/glukhin-v-russia-the-european-court-of-human-rights-first-step-into-the-age-of-ai-surveillance/>accessed January 22nd, 2026.

[4] European Data Protection Board "The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC" < https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en>(accessed January 22, 2025)

[5] Centre for Information Policy Leadership "*Decoding Responsibility in the Era of Automated Decisions: Understanding the Implications of the CJEU's SCHUFA Judgment*" <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_decoding_responsibility_automated_decision_making_oct24.pdf> (Accessed January 22nd,2026)

[6] Section 37(3) of the NDPA.