

EU AI Act:

Prohibited Practices for Nigerian Developers

Introduction

The European Union Artificial Intelligence Act (“the EU AI Act” or “the Act”) entered into force on August 1, 2024,¹ establishing the world's first comprehensive legal framework for regulating artificial intelligence. Critically, the Act has extraterritorial reach: any developer whose AI system produces output used within the EU falls within its regulatory scope, regardless of the developer's physical location.²

Nigerian AI developers increasingly build products serving global users across fintech, edtech, health tech, and security, many of which directly target European markets or have users within the EU. For these developers, compliance with the EU AI Act is a commercial and legal imperative. This article examines the eight prohibited AI practices under Article 5, analyses their practical implications for Nigerian developers, and outlines a route toward compliance.

The EU AI Act: A Brief Overview

The Act adopts a **risk-based approach**, classifying AI systems into four tiers: unacceptable risk (prohibited), high risk (heavily regulated), limited risk (transparency obligations), and minimal risk (largely unregulated).³ The key actors are “providers” (those who develop or bring AI systems to market) and “deployers” (those who use AI systems professionally). Both providers and deployers outside the EU are subject to the Act where the output of their AI systems is used within the Union.⁴

Unacceptable Risk — **Prohibited**

High Risk — **Heavily Regulated**

Limited Risk — **Transparency**

Minimal Risk — **Largely Unregulated**

The Eight Prohibited AI Practices Under Article 5

Article 5 establishes eight categories of AI practices that pose an unacceptable risk and are entirely prohibited.⁵ These prohibitions took effect on 2 February 2025, and the European Commission has issued guidelines clarifying their scope.⁶

01 Subliminal, Manipulative, and Deceptive AI Systems:

The Act prohibits AI systems that deploy subliminal techniques or purposely manipulative or deceptive techniques with the objective or effect of materially distorting behaviour and impairing informed decision-making, thereby causing, or being reasonably likely to cause, significant harm.⁷ For Nigerian developers, this encompasses marketing automation tools that use dark patterns, betting platforms that exploit behavioural data to encourage compulsive wagering, and recommendation engines designed to maximise addictive usage.

02 Exploitation of Vulnerabilities:

AI systems that exploit vulnerabilities arising from age, disability, social or economic circumstances to materially distort behaviour in a manner causing or likely to cause significant harm are prohibited.⁸ A lending application targeting financially distressed individuals with predatory loan offers would likely violate this provision.

03 Social Scoring Systems:

AI systems that evaluate or classify persons based on social behaviour or personal characteristics are prohibited where such scoring leads to detrimental treatment in unrelated social contexts, or treatment that is unjustified or disproportionate.⁹ A fintech developer whose algorithm aggregates social media activity and spending habits to generate a “trustworthiness score” affecting access to housing or employment would operate in prohibited territory.

04 Predictive Criminal Profiling:

The Act prohibits AI systems that assess or predict the risk of criminal offending based solely on profiling or personality assessments.¹⁰ However, AI systems supporting human assessment based on objective, verifiable facts directly linked to criminal activity remain permissible. Nigerian developers building security solutions must ensure their systems do not cross into speculative profiling.

The Eight Prohibited AI Practices Under Article 5

05 **Untargeted Facial Image Scraping:**

The creation or expansion of facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage is prohibited.¹¹ Nigerian developers building identity verification platforms must ensure their training data is lawfully acquired and that their systems do not engage in mass, untargeted collection of facial images.

06 **Emotion Recognition in Workplaces and Educational Settings:**

AI systems that infer the emotions of persons in workplace and educational settings are prohibited, except where the system serves medical or safety purposes.¹² This directly affects Nigerian edtech developers who incorporate engagement-tracking features and HR technology firms that use AI to assess employees' emotional states.

07 **Biometric Categorisation for Sensitive Attributes:**

AI Systems that categorise persons based on biometric data to deduce or infer race, political opinions, trade union membership, religious beliefs, sex life, or sexual orientation are prohibited.¹³ Nigerian developers working on biometric solutions must ensure their systems do not classify individuals based on these characteristics.

08 **Real-Time Remote Biometric Identification in Public Spaces:**

Real-time remote biometric identification in publicly accessible spaces for law enforcement is generally prohibited, subject to narrow exceptions requiring prior judicial or administrative authorisation.¹⁴ Nigerian developers providing such solutions to law enforcement agencies within the EU must be aware of these constraints.

Practical Implications for Nigerian AI Developers

Several common Nigerian AI use cases carry a real risk of non-compliance. In fintech, credit scoring algorithms that incorporate social media behaviour or psychometric assessments may constitute social scoring, while lending platforms targeting vulnerable populations risk engaging in exploitation. In edtech, platforms incorporating emotion detection to measure student engagement are directly caught by the emotion recognition prohibition. In recruitment technology, AI tools that assess candidates through personality profiling or emotional analysis may violate multiple prohibitions simultaneously. In security and surveillance, facial recognition systems trained on scraped internet images and predictive policing tools fall squarely within the prohibited categories.

*A single product can simultaneously trigger **two or more** Article 5 prohibitions — the analysis is functional, not nominal.*

Enforcement and Penalties

Violations of Article 5 attract administrative fines of up to EUR 35 million, or up to 7% of the offending undertaking's total worldwide annual turnover, whichever is higher.¹⁵ Enforcement authorities may also order the withdrawal of non-compliant AI systems from the market. The AI Office within the European Commission exercises overarching supervisory functions, while national competent authorities handle domestic enforcement.¹⁶ For small and medium-sized enterprises, the Act provides that penalties must be proportionate, taking into account economic viability,¹⁷ though this does not eliminate the risk but merely modulates its quantum.

ADMINISTRATIVE FINE

€**35**m

Maximum fine for Article 5 violations

OR (WHICHEVER IS HIGHER)

7%

of total worldwide annual turnover of the offending undertaking

Intersection with the Nigerian Regulatory Framework

Nigerian AI developers do not operate in a regulatory vacuum domestically. The Nigeria Data Protection Act 2023¹⁸ shares conceptual ground with the GDPR and certain principles underpinning the EU AI Act. The Federal Ministry of Communications, Innovation and Digital Economy, working with NITDA, has published a National Artificial Intelligence Strategy.¹⁹ Sector-specific regulators, including the Central Bank of Nigeria for fintech and the Nigerian Communications Commission for telecommunications, impose obligations that intersect with AI governance. A holistic compliance framework addressing both jurisdictions is more efficient than treating each regime in isolation.

i. Nigeria Data Protection Act 2023

Shares conceptual ground with the GDPR and certain principles underpinning the EU AI Act.

ii. National Artificial Intelligence Strategy

Published by the Federal Ministry of Communications, Innovation and Digital Economy, working with NITDA.

iii. Sector-Specific Regulators

The CBN (fintech) and NCC (telecommunications) impose obligations that intersect with AI governance.

A Compliance Roadmap for Nigerian Developers

Nigerian AI developers seeking compliance with the Act's prohibited practices provisions should consider several key steps: conducting an AI system audit against Article 5 criteria, mapping each system's functionality against the eight prohibited categories; embedding compliance at the design stage through legal review during development and testing; maintaining documentation of AI systems' intended purposes, technical specifications, and training data sources; monitoring EU market exposure by tracking whether systems or outputs are consumed within the Union; and engaging legal and compliance expertise to navigate the Act's interaction with existing data protection and sector-specific regulations.

Conclusion

The EU AI Act represents a paradigm shift in AI governance. Its extraterritorial reach ensures that Nigerian AI developers cannot treat it as a foreign concern. The eight prohibited practices under Article 5 establish clear boundaries, and the penalties for violation are severe. For Nigerian developers, however, the Act should be viewed not merely as a compliance burden but as a competitive opportunity. Developers who align their products with its requirements will be better positioned to access the European market, attract international investment, and build global trust.

Notably, compliance with a foreign regulatory framework is not substitute for homegrown governance. Nigeria must move toward a coherent, enforceable AI framework of its own. The Nigeria Data Protection Act 2023 and the National AI Strategy 2024 provide a foundation, but neither addresses the full spectrum of risks that AI systems pose to Nigerian consumers, businesses, and public institutions.

What Nigeria requires is a legal framework that draws on international best practices while remaining responsive to Nigeria's unique economic realities and institutional capacity.

The cost of inaction is that Nigeria's rapidly growing technology sector will be governed by rules written elsewhere, for contexts other than its own.

THE COST OF INACTION

Nigeria's rapidly growing technology sector will be governed by rules written elsewhere, for contexts other than its own.

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689.
2. *ibid* art 2(1)(c).
3. *ibid* art 6. High-risk AI systems are subject to mandatory requirements under ch III, s 2.
4. *ibid* recital 24.
5. Artificial Intelligence Act, art 5. The prohibitions under art 5 took effect on 2 February 2025, being six months after the Act's entry into force on 1 August 2024: see art 113(a).
6. European Commission, 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689' (4 February 2025).
7. Artificial Intelligence Act, art 5(1)(a).
8. *ibid* art 5(1)(b).
9. *ibid* art 5(1)(c). The prohibition extends to treatment that is detrimental in social contexts unrelated to the contexts in which the data was originally generated or collected.
10. *ibid* art 5(1)(d).
11. *ibid* art 5(1)(e). See also recital 43 of the EU AI Act, which explicitly references the scraping of facial images from the internet or CCTV as the type of practice targeted by this prohibition.
12. *ibid* art 5(1)(f).
13. *ibid* art 5(1)(g).
14. *ibid* art 5(1)(h). Narrow exceptions apply for specific law enforcement purposes, subject to prior judicial or administrative authorisation: see art 5(2).
15. *ibid* art 99(3).
16. *ibid* arts 64–68, establishing the AI Office within the European Commission.
17. *ibid* art 99(5).
18. Nigeria Data Protection Act 2023. The Act received Presidential assent on 12 June 2023 and was published in the Federal Republic of Nigeria Official Gazette, No 37, Vol 110, 1 July 2023.
19. Federal Ministry of Communications, Innovation and Digital Economy and National Information Technology Development Agency (NITDA), 'National Artificial Intelligence Strategy' (Draft, August 2024) https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf accessed 5 February 2025.

Contributors

12



Okechukwu Ekweanya

Partner, TMT



Elizabeth Aghaulor

Associate, TMT



Olusola Odeku

Associate, TMT



CONTACT US

LAGOS

KENNA Place
8, Ogunyemi Road, Palace Way, Oniru
PO Box 73002, Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285, Abuja

ENUGU

Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner,
400211 Enugu State.

+234 811 395 1052, +234 811 395 1053
counsel@kennalp.com