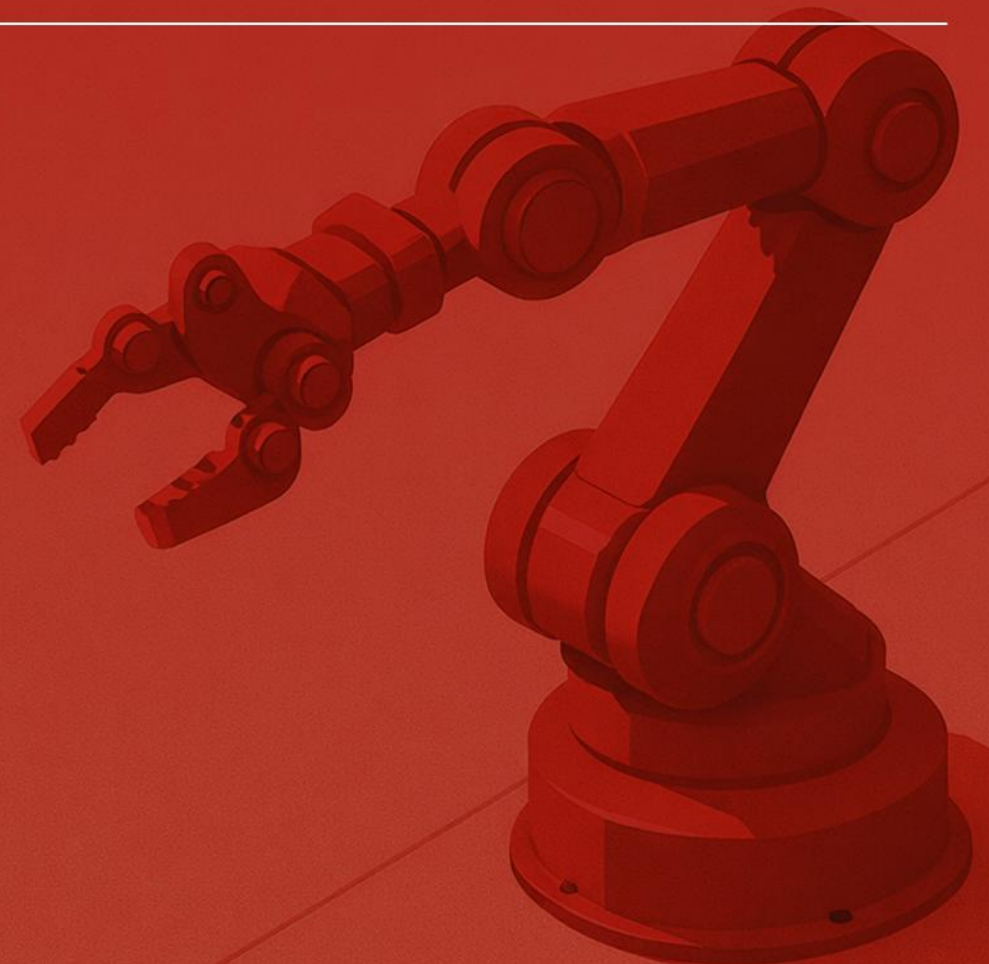


Data Privacy, Consent and Corporate Accountability in the Age of Generative AI



WIGWE & PARTNERS

JULY 2026



MAGE | THOUGHT LEADERSHIP

IN THIS ARTICLE

Introduction

Principal Legal Frameworks for Data Privacy in Nigeria

Data Privacy Risks on Generative AI

Consent Conundrum in AI system

Corporate Accountability in the AI era

Conclusion

WIGWE & PARTNERS

AUTHORS



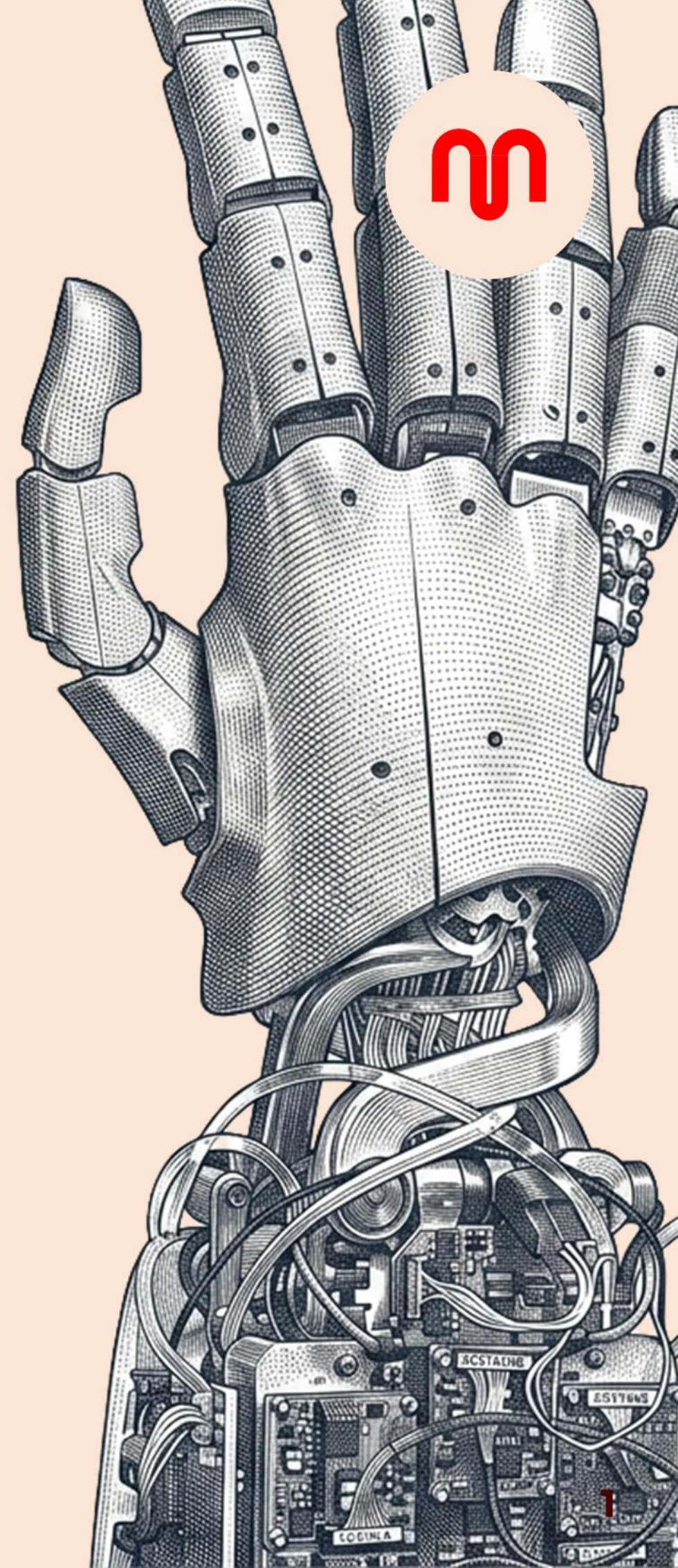
Godswill
Emmanuel

Associate



Chukwunonso S.
Ndukwe

Associate



INTRODUCTION

Generative Artificial Intelligence (GenAI) is the branch of AI that learns the patterns, structure, and relationships within massive datasets and uses this knowledge to produce original content in response to prompts or queries.¹ This is unlike traditional AI, which merely attempts to distinguish or predict categories within existing data.²

The rapid use of GenAI has proved beneficial in this age of digital technology by enhancing creativity and innovation across different sectors. However, its deployment also raises pressing legal and regulatory concerns especially

as regards to processing of personal data, the adequacy of data subject's consent, and the potential infringement of privacy rights by corporate entities which leverage AI systems.

In view of the foregoing, this article addresses the growing relationship between GenAI, data privacy, consent, and corporate accountability. It examines the legal and regulatory frameworks regulating the processing of personal data in AI systems, the challenges associated with informed consent, and the extent to which corporate entities are responsible for ensuring compliance with data protection laws

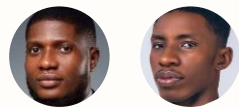
PRINCIPAL LEGAL FRAMEWORKS FOR DATA PRIVACY IN NIGERIA

1. Constitution of the Federal Republic of Nigeria (CFRN) 1999: The CFRN 1999 is the principal enactment that establishes data privacy rights in Nigeria. It provides that the privacy of citizens, their homes, correspondence, telephone communications and telegraphic communications is hereby guaranteed and protected.³ The CFRN does not define privacy. However, in line with the “living tree”⁴ doctrine of constitutional interpretation the right to privacy should not be construed narrowly. Rather, it should be interpreted broadly, encompassing a wide range of interests and protections relating to an individual's private life, and must be capable of adapting to new technological developments that continually reshape the ways in which personal information is collected, stored, and used.

2. Nigeria Data Protection Act (NDPA) 2023: The NDPA 2023 was signed into law by President Bola Ahmed Tinubu on 14th June, 2023.⁵ It makes notable provisions for the protection of personal data and is the first law signed by a legislative body that specifically addresses the protection of personal data in Nigeria.⁶ The Act seeks to safeguard the fundamental rights of data subjects by establishing a regulatory framework for the processing of personal data, promoting secure and responsible data processing practices, and ensuring that data subjects have access to effective remedies and avenues for redress where their rights are infringed.⁷

¹ Saran, RK, 'Evolution of Generative AI: Shaping Tech Solutions', (Entrans, 24 January, 2025) <Evolution of Generative AI: Shaping Tech Solutions> accessed 9 June, 2026.
² Bartlett, I, et al, 'The Rise of Generative AI: Opportunities and Challenges', (Ox Journal, 20 August, 2025) <The Rise of Generative AI: Opportunities and Challenges (I) | OxJournal> accessed 9 June, 2026
³ CFRN 1999, s 37.
⁴ This doctrine requires that the Constitution be read as a dynamic instrument capable of growth to meet evolving societal needs. See N.U.P. v. I.N.E.C. (2021) 17 NWLR (Pt. 1805) 305
⁵ Ndinojuo, BE, and Peter, DI, 'Privacy Awareness and Social Media: Privacy Data Protection Among Facebook and Instagram Users', (Research Gate, September, 2024), '<(PDF) Privacy Awareness and Social Media: Personal Data Protection among Facebook and Instagram Users> accessed 9 June, 2026.
⁶ Ibid.
⁷ NDPA 2023, s 1.

WIGWE & PARTNERS



The NDPA 2023 also provides for the rights of data subjects, including the right to access information⁸ with respect to the processing of their personal information, right to withdraw consent,⁹ right to object to certain forms of processing,¹⁰ and exercise rights relating to automated decision-making¹¹ and data portability.¹² These rights ensure that transparency and accountability are promoted, individuals exercise some form of control over their personal data, and that data controllers and processors act responsibly in handling personal information of data subjects. Finally, the Act establishes the Nigeria Data Protection Commission (NDPC)¹³ to administer and ensure that adequate measures are put in place for the protection of personal data.¹⁴

3. General Application and Implementation Directive (GAID) 2025: The NDPA 2023 is further complemented by the GAID 2025, a Directive issued by the NDPC. Further to the substantive rights provided for by the NDPA, the GAID provides practical guidance on the implementation and enforcement of those provisions. Thus, the Directive poses as the practical framework through which data controllers and data processors ought to show compliance with the Act.

The provisions of the Directive relevant to GenAI include provisions relating to Compliance Audit Returns,¹⁵ Data Privacy Impact Assessments (DPIAs),¹⁶ data breach notifications,¹⁷ among others. Together, these provisions are aimed at ensuring that organizations adopt a proactive and accountable approach to data protection. These measures require data controllers and processors to regularly assess their compliance status and promptly report data breaches to the relevant authorities and affected data subjects where necessary.

4. Sector-Specific Regulations: Away from the CFRN 1999 and the NDPR 2023, Nigeria's data privacy legal system is regulated by other sector-specific laws in various industries such as the National Health Act 2014, for the healthcare sector, and the Nigerian Communications (Consumer Code of Practice) Regulations 2024, for the telecommunications, among others. These regulations impose obligations on entities in these respective sectors and contribute collectively to the protection of personal data in Nigeria.

DATA PRIVACY RISKS ON GENERATIVE AI

GenAI has sparked a transformative wave across various domains, including machine learning, healthcare, entertainment, and business, owing to its remarkable ability to generate lifelike data.¹⁸ The use of GenAI has introduced a range of complex privacy risks¹⁹ that goes beyond those associated with traditional data processing systems. These systems are trained on a large amount of and diverse datasets, including personal data sourced from multiple platforms, usually without the knowledge of the individuals concerned.

This has equally led to major AI developers being sued.²⁰ It was reported in 2023, for instance, that Meta trained its large language model (LLM) in part on a dataset called Books, which contained more than 170,000 pirated and copyright books.²¹ This spark concerns about lawful basis for data processing and compliance with purpose limitation principle, especially where data collected for one purpose is thereafter used for training AI and model development.

⁸ Ibid, s 34.

⁹ Ibid, s 35.

¹⁰ Ibid, s 36.

¹¹ Ibid, s 37.

¹² Ibid, s 38.

¹³ Ibid, s 4.

¹⁴ Ibid, S5

¹⁵ GAID, art 17.

¹⁶ Ibid art 28

¹⁷ Ibid art 33

¹⁸ Golda, A, et al, 'Privacy and Security Concerns in Generative AI: A Comprehensive Survey', (Research Gate, January 2024), <(PDF) Privacy and Security Concerns in Generative AI: A Comprehensive Survey> accessed 9 June, 2026.

¹⁹ Diro, A, et al, 'Workplace Security and Privacy Implications in the GenAI Age: A Survey', (2025)(29) Journal of Information Security and Applications', < Workplace security and privacy implications in the GenAI age: A survey – ScienceDirect > accessed 9 June, 2026> accessed 9 June, 2026.

²⁰ Leffer, L, 'Your Personal Information is Probably Being used to Train Generative AI Models', (19 October, 2023), <Your Personal Information is Probably Being Used to Train Generative AI Models | Scientific American

²¹ Ibid.

WIGWE & PARTNERS



Additionally, GenAI systems unintentionally memorize and replicate personal information contained within training data²² and this leads to unintended disclosures through user prompts. The opaque nature of many AI models further worsens these risks since data subjects or even

organizations may lack the clear understanding of how data is processed. Hence, these challenges conjunctively pinpoint emerging security and accountability concerns within the existing data protection framework.

CONSENT CONUNDRUM IN AI SYSTEM

The NDPA 2023 defined consent as any freely given, specific informed, and unambiguous indication whether by a written or oral statement or an affirmative action, of an individual's agreement to the processing of personal data relating to him or to another individual on whose behalf he has the permission to provide such consent.²³

As seen above, consent has to be informed and freely given as the data subject possesses the right not to subject to a decision based solely on automated processing of personal data, including profiling which produces legal or similar significant effects concerning the data subject.²⁴

However, problem as to consent arises where data subjects are unaware of the fact that their data are used for training AI. That is to say, secondary usage of their data is not clearly disclosed which undermines the validity of consent as laid down in the NDPA. Also, companies often rely on their legitimate intention of the usage of the data to justify the appropriateness of the secondary usage of the data without explicit consent. Against the backdrop of the NDPA, this raises a dilemma as to the point where consent can seem to be withdrawn or the extent of the consent given by a data subject on its data usage

CORPORATE ACCOUNTABILITY IN THE AI ERA

Pointedly, the NDPA is built on the principle of accountability. Thus, the obligations of organizations transcend beyond complying with rules without more, and incorporates the idea that they are required to demonstrate, document, and prove that they are complying with all data protection obligations when processing personal data.²⁵

In addressing the issue of accountability, it becomes pertinent to understand who a data controller/processor is. The Act defines a data controller as an individual, private entity, or any other body who determines the purposes and means of processing of personal data.

On the other hand, a data processor is an individual, private entity or other persons who processes personal data on behalf of or at the direction of a data controller or another data processor. Thus, corporate entities that determine the purposes and means of processing personal data, or process such data on behalf of others, fall within the ambit of the Act and are subject to its accountability and compliance obligations.

The Act set out the obligations of the data controller and data processor to ensure the security, integrity and confidentiality of data in the possession of the data controller or

²² Sajid, H, 'The Growing Threat of Data Leakage in Generative AI Apps', (Unite AI, 13 May, 2024), <-The Growing Threat of Data Leakage in Generative AI Apps Unite.AI> accessed 9 June, 2026

²³ NDPA 2023, s 65.

²⁴ NDPA 2023, s 37.

²⁵ Ikeh, J, 'Accountability Principle under the Nigeria Data Protection Act (NDPA)', Privacy Needle <Accountability Principle Under the Nigeria Data Protection Act (NDPA) – Privacy Needle> accessed 11th June, 2026.

WIGWE & PARTNERS



processor.²⁶ The Act further provides that a data controller and data processor are vicariously liable for the acts or commissions of its agent or employees, in so far as it relates to its business.²⁷

This proves that the evasion of liability for corporate organizations is futile as the NDPA

2023 and the General Application and implementation directive (GAID) 2025 holds them accountable for the data in their possession. As such, the onus is on them to get informed consent before the procession of data while maintaining the integrity and confidentiality of same.

²⁶ NDPA 2023, s 29.
²⁷ Ibid, s 53(2).

CONCLUSION

While Generative AI is beneficial for rapid developments and innovations in our society today, attention must be paid to the usage of data for training this AI models. Corporate organizations must take into account that Informed consent of data subjects must be

sought before processing. Data protection impact assessment (DPIA) must be made to ascertain the data privacy risks that might be involved in the usage of these data to avoid liability as imposed by the NDPA 2023 and GAID 2025.

