



CHALLENGES TO THE PROTECTION AND ENFORCEMENT OF PRIVACY RIGHTS OF NIGERIAN WORKERS UNDER THE NIGERIAN DATA PROTECTION ACT 2023

Osigwe, Billy Ademi*
Kpea-Ue, Bariyira Simple**

ABSTRACT

The Nigerian Data Protection Act, 2023 represents a landmark legislative intervention aimed at safeguarding the fundamental right to privacy under Section 37 of the 1999 Constitution while regulating the processing of personal data in an increasingly digital economy. Through a doctrinal legal analysis of the Act's objectives, this study evaluates the extent to which the NDPA strengthens protections against workplace surveillance, biometric data collection, HR record retention, cross-border transfers of employee data, and automated decision-making in recruitment or performance evaluation. This study appraises the NDPA's provisions in the specific context of workers' rights, examining how the Act balances employers' operational needs with employees' data privacy interests in the employment relationship. The appraisal reveals notable strengths: the introduction of legitimate interest as a lawful basis, enhanced accountability and security obligations on data controllers and processors, mandatory data protection impact assessments for high-risk processing, and robust rights to access, rectification, erasure, objection, and (prospectively) portability. These provisions empower workers as data subjects and impose clear obligations on employers. However, critical gaps persist. The Act lacks specific rules on workplace monitoring (for example, CCTV, email surveillance, or GPS tracking), relies on consent in a context where power imbalances undermine its voluntariness, and does not expressly address collective worker rights or the interplay with labour legislation. Enforcement challenges and the absence of detailed subsidiary regulations further limit its efficacy. This study concludes that while the NDPA marks a progressive shift from the Nigeria Data Protection Regulation 2019, and recommends targeted regulatory guidelines from the Nigeria Data Protection Commission (NDPC) and possible legislative amendments are essential to fully realise its protective potential for Nigerian workers.

Keywords: Workers, Data, Rights, Privacy

1. INTRODUCTION

Nigeria's digital transformation has profoundly reshaped the employment landscape, with employers routinely processing vast amounts of workers' personal data from recruitment platforms and biometric attendance systems to electronic monitoring of emails, internet usage, CCTV footage, and performance analytics. This pervasive datafication raises acute privacy concerns, particularly given the inherent power imbalance in the employer-employee relationship. Prior to 2023, data protection in Nigeria rested primarily on the Nigeria Data Protection Regulation 2019 (NDPR), a non-statutory instrument lacking robust enforcement mechanisms. The enactment of the Nigerian Data Protection Act¹ fills this vacuum by establishing a comprehensive statutory

* LLB (RSUST), BL (Abuja), LLM (RSU), PhD (In-view), billyosigwe@yahoo.com; +2347064774524

** OND, B.SC(Hons.), LL.B(First Class), LL.M(RSU), B.L (Abuja), PhD (Nigeria), Lecturer, Department of Private and Property Law, Faculty of Law, Rivers State University, Nkpolu-Oroworukwo, Port-Harcourt.



framework and an independent Nigeria Data Protection Commission (NDPC). The enactment of the NDPA marks a significant milestone in Nigeria's data protection, as it establishes a comprehensive legal framework for regulating the collection, use, and safeguarding of personal data. Employment relationships between employer and employee often require workers to disclose sensitive information such as biometric data, health records, and financial details. The NDPA has direct relevance for protecting workers' privacy and ensuring fairness at workplace. This study interrogates whether the Act adequately safeguards employees' data privacy while accommodating legitimate business interests and identifies challenges against effective enforcement in Nigeria.

2. LEGAL APPRAISAL OF THE PROVISIONS OF THE NIGERIAN DATA PROTECTION ACT 2023 AS IT RELATES TO WORKERS

The enactment of the NDPA represents a significant development in the regulation of personal data in Nigeria, particularly as it concerns workers. Employment relationships inherently require employees to disclose sensitive information such as biometric data, health records, financial details, and performance metrics.² Through the recognition of employers as data controllers, the NDPA extends constitutional protections under section 37 of the 1999 Constitution (as amended), which guarantees the privacy of citizens, to the workplace. Judicial decisions such as *Eneye v MTN Nigeria Ltd and Anene v. Airtel Nigeria Ltd*³ affirm this constitutional right by recognising that the unauthorised disclosure of personal data constitutes a breach of privacy. In this way, the NDPA reinforces privacy as a fundamental right of workers.

The Act applies to all entities engaged in the processing of personal data in Nigeria, including employers who qualify as data controllers. Under section 25 of the NDPA, data processing must be based on lawful grounds such as consent, contractual necessity, or legitimate interest.⁴ This provision ensures that employers cannot arbitrarily collect or retain employee data without legal justification. Workers, as data subjects, are also granted rights of access, rectification, erasure, and objection to processing. Section 31 of the Act empowers employees to demand correction of inaccuracies in their records, while section 33 permits them to challenge intrusive practices such as unwarranted surveillance or profiling.⁵

Employers are bound by several obligations under the Act. There is the duty to obtain informed consent for processing data not strictly required for contractual or statutory purposes. For example, the processing of health data beyond occupational safety requirements must be grounded in explicit consent. Larger organizations are mandated under section 32 to appoint Data Protection Officers to ensure compliance and accountability. Employers must also adopt technical and organizational

baryira.kpea-ue@ust.edu.ng +2348068753214.

¹ Nigerian Data Protection Act 2023 (Hereinafter NDPA).

² D Chika and E Tochukwu, 'An Analysis of Data Protection and Compliance in Nigeria' [2020] (4) (5) *International Journal of Research and Innovation in Social Science*, 377 - 382.

³ *Godfrey Nya Eneye v MTN Nigeria Communication Ltd Appeal* No. CA/A/689/2013 (Unreported).

⁴ Chika and Tochukwu (n 2) 379.

⁵ I Odekina and Others, 'Guide to Data Protection in Nigeria' (2020) *Commercial and Energy Law Practice*, 20.



measures to safeguard employee data against breaches. Failure to do so attracts both administrative sanctions and potential liability in damages.⁶

Oversight is entrusted to the NDPC established under section 3 of the NDPA. The Commission is empowered to register data controllers, monitor compliance, and sanction offenders. In principle, this enhances workplace data protection, but questions remain regarding the Commission's institutional capacity to regulate Nigeria's vast and diverse employment sector.⁷ The challenge of enforcing compliance across both public and private sectors, particularly among SMEs, underscores the importance of proactive regulatory strategies. Comparative jurisprudence provides useful lessons. For instance, in *Barbulescu v Romania*,⁸ the European Court of Human Rights ruled that excessive workplace surveillance violated the right to privacy. This highlighted the need for courts to balance employer interests with employee dignity. Nigerian courts, when confronted with similar disputes, may draw from such reasoning in interpreting the NDPA alongside section 37 of the Constitution.

3. SAFEGUARDING THE FUNDAMENTAL RIGHTS AND FREEDOM OF NIGERIAN WORKERS UNDER NIGERIAN DATA PROTECTION ACT 2023

Data protection and privacy is an extension of the fundamental right of workers to privacy. Section 37 of the 1999 Constitution⁹ protects the rights of workers to their privacy and the privacy of their homes, correspondence, telephone conversations and telegraphic communication. Aside from the Constitution, there are several other legislation that contain such protective provisions. For instance, the Freedom of Information Act¹⁰ enables public access to public records and information, prevents a public institution from disclosing personal information to the public unless the worker involved consents to the disclosure. The Cybercrimes (Prohibition, Prevention, etc) Act¹¹ prevents the interception of electronic communications and imposes data retention requirements on financial institutions.¹² The Consumer Code of Practice Regulations¹³ issued by the Nigerian Communications Commission requires telecommunication operators to take reasonable steps to protect against "improper or accidental disclosure" and must ensure that such information is securely stored. It also provides that customer information must "not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations."¹⁴ The Consumer

⁶ D Nnam, 'Informational Privacy and Security Amid Growing Activities on Electronic Platforms in Nigeria: A Case for Data Protection Law' [2015] *NAUJILJ*, 27 - 33.

⁷ A Akindele, 'Data Protection in Nigeria: Addressing the Multifarious Challenges of a Deficient Legal System' [2017] (26) (4) *Journal of International Technology and Information Management*, 110 – 125.

⁸ *Bărbulescu v Romania* App. No. 61496/08, Grand Chamber Judgment, 5 Sept 2017, [2017] ECHR 754.

⁹ Constitution of the Federal Republic of Nigeria 1999 (as amended), Cap C23, LFN 2004 (CFRN).

¹⁰ Freedom of Information Act No. 4 of 2011.

¹¹ Cybercrime (Prohibition, Prevention etc.) Act No. 17 of 2015 (CCPPA 2015).

¹² *Ibid*, s 1.

¹³ Consumer Code of Practice Regulations 2007.

¹⁴ A Adeyoju, 'A Quick Guide on the Data Protection Regime in Nigeria' <https://ilca.africa/wp-content/uploads/2020/05/ADEMOLA_ADEYOJU-A-Quick-Guide-on-the-Data-Protection-Regime-in-Nigeria_compressed.pdf> accessed 6 May 2025.



Protection Framework issued by the Central Bank of Nigeria in 2016 contains provisions that restrain financial institutions from disclosing the personal information of their customers. It has however been evident that though these preceding pieces of legislation exist, there had been no comprehensive data protection and data privacy legislation in Nigeria.

4. LEGAL ANALYSIS OF THE RIGHTS OF WORKERS

A legal analysis of the rights of workers is essential to understanding how the Constitution envisages the balance between the prerogatives of employers and the fundamental rights of employees.

4.1 Fundamental Rights

Under the 1999 Constitution,¹⁵ the right to privacy is recognised as a fundamental right in the following words: ‘The privacy of *workers*, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected.’ With this express provisions, it is ostensible that the Constitution drafters clearly intended and sought expressly to prohibit any infringement of workers’ rights to bodily, communications, and territorial privacy. What is not as apparent or is at best arguable, from the provisions of the Constitution, is the recognition of the right of workers to data protection.

The CFRN does not, however, provide the meaning of privacy within the scheme of fundamental human rights. Nwauche,¹⁶ gives some insights into the meaning of privacy as envisaged by the Constitution. He observes that there could be a general and specific understanding of privacy based on the constitutional provision: Accordingly, the use of the word ‘the privacy of workers’ constitutes the general right in this section. Thus, the use of the words ‘...their homes, correspondence, telephone conversations and telegraphic communications...’ are the specific enumerations of the aforesaid general right.¹⁷

In the same vein, Allotey,¹⁸ argues that the reference by the Constitution to citizen’s correspondence, their telephone and telegraphic communications envisages an intention to protect information privacy which involves protection of a worker against unlawful interference with his personal information held by other workers. The scope of information privacy covers collection, storage, usage, and dissemination of personal information by both public and private bodies.¹⁹ The 1999 CFRN, therefore partially guarantees data privacy based on the scope of the right to privacy.

¹⁵ CFRN 1999 (n 9), s 37.

¹⁶ E S Nwauche ‘The Right to Privacy in Nigeria’ (2007) (1)(1) *Review of Nigerian Law and Practice*, 84.

¹⁷ Adeyoju (n 14)

¹⁸ A Ake, ‘Data Protection and Transborder Data Flows: Implication for Nigeria’s Integration into the Global Network Economy’ Unpublished LLD Thesis, University Of South-Africa In 2014, 173.

¹⁹ Ake (n 15), 173.



Information privacy is only an aspect of the law on data privacy and therefore, it cannot be said that a worker's right to data privacy is effectively guaranteed by the constitutional provision.²⁰

Nigeria implemented the Data Protection Regulation (the "NDPR") in 2019 to control the collection and processing of Personal Data of Natural Workers in Nigeria, continuing the global trend towards data privacy and protection.²¹ There has emerged a debate amongst privacy rights activists and data protection enthusiasts regarding the relationship that exists between the rights of a Data Subject under the NDPR and the privacy rights guaranteed under the CFRN specifically, the debate is whether the rights of the Data Subject under the NDPR may be subsumed under the right to privacy provided in the Constitution, such that the Data Subject, whose rights under the NDPR have been breached may enforce these rights by way of an action brought under the Fundamental Rights (Enforcement Procedure) Rules.²² The extant FREP Rules were enacted on 1 December 2009²³ under the authority of section 46(3)²⁴ of the Constitution and prescribe the procedure for the enforcement of fundamental rights enshrined in Chapter IV of the Constitution as well as the fundamental rights provided for under the African Charter on Human and People's Rights.²⁵

Some data protection enthusiasts have argued that the rights of the Data Subject under the NDPR are analogous to the right to privacy under section 37 of the Constitution and as such, those rights can be enforced in the same way fundamental rights guaranteed under the Constitution may be enforced. The proponents of this view contend that the Data Subject's rights under the NDPR are a specie of the right to privacy under section 37 of the Constitution and to that extent, those rights are enforceable the same way the privacy right may be enforced. This contention recently found support in the decision of the Ogun State High Court presided over by the Honourable Justice O. Ogunfowora, in *Incorporated Trustees of Digital Rights Lawyers Initiative v. L.T Solutions & Multimedia Limited*²⁶ where it was held that a Data Subject's rights under the NDPR may be enforced the same way a Constitutional right is enforced under the FREP Rules.

The approach adopted by the court, in this case, tends to suggest that a breach of a Data Subject's right under the NDPR may be remedied by an action brought under the FREP Rules simpliciter. On the flip side, those opposed to this view, however, argue that a Data Subject's rights under the NDPR are neither constitutional rights nor fundamental human rights under the African Charter,

²⁰ D W Schartum 'Designing and formulating data protection laws' (2008) (18) *International Journal of Law and Information Technology*, 56.

²¹ Templars, 'Enforcing Data Subjects Rights under Nigeria's Data Protection Regulation: The Wrong way (The Right way)' <<https://www.templars-law.com/wp-content/uploads/2021/01/Templars-Thought-Leadership-Publication-on-Enforcing-Data-Subject-Rights-Under-Nigeria%E2%80%99s-Data-Protection-Regulation-The-Wrong-Way-And-The-Right-Way.pdf>> accessed 19 June 2025.

²² Fundamental Rights (Enforcement Procedure) Rules 2009.

²³ Fundamental Rights (Enforcement Procedure) Rules 2009.

²⁴ CFRN 1999 (n 9), s 46(3).

²⁵ African Charter on Human and Peoples' Rights (Ratification and Enforcement) Act, Cap. A9 LFN, 2004 (ACHPR Act).

²⁶ Suit No. AB/83/2020 (Unreported).



and as such, cannot be enforced under the procedure provided in the FREP Rules. This position received judicial approval in the recent judgment of the Federal High Court of Nigeria (the “FHCN”) presided over by the Honourable Justice Ibrahim Watila delivered on 9 December 2020 in the case between *The Incorporated Trustees of Laws and Rights Awareness Initiative v. The National Identity Management Commission*²⁷ (RAI vs NIMC). It was held in the case that a breach of Data Subject’s right under the NDPR is not necessarily a breach of the right to privacy under the Constitution, so a claim for interpretation of the provisions of the NDPR is not a fundamental rights action falling within the purview of the FREP Rules.

In EU, the right to data protection is a fundamental right recognized by the Charter of Fundamental Rights of the European Union 2000 and constitutional laws of many member States, as well as the case law of European Court of Justice (ECJ). The exercise of this right and the enforcement of the incurred duties and responsibilities of data controllers and processors that process various personal data of EU residents, become critically important in the context of increasing digitalization and connectedness of our globalized economy and community.²⁸ As a leading comprehensive legislation in the field, the European General Data Protection Regulation (GDPR) aims to not only facilitate data flows within the EU,²⁹ but also concretizes and materializes, for the first time in a systematical way, this right by means of granting a group of specific rights (to data subjects) and protecting them through establishing a strict law implementation mechanism. This includes the rights to access, information, objection, data portability, explicit consent (and withdrawal of consent), data rectification, data erasure (the right to be forgotten), remedy, and so on. More importantly, GDPR claims protection of all data subjects that reside in the EU, regardless of their nationalities, and regulates cross-border data transfers towards non-EU countries, thus being applicable to the controllers and processors that are not on EU territory, but process personal data of natural workers in EU. There have been, however, rising doubts over the protection of the fundamental right in the context of extraterritorial application of the related GDPR rule.³⁰

4.2 Inappropriate Disclosure of Personal Information

Although The NDPR does not specifically provide any criminal liabilities and sanctions for violators of the Regulation, it only in Article 2.10 of the said Regulation provide to the effect that any worker subject to this Regulation who is found to be in breach of the data of the privacy rights of any Data Subject shall be liable, in addition to any other criminal liability. The said Regulation went further in Article 4.3 (6) of the Regulation to provide that any breach of the said regulation shall be construed as a breach of the provisions of the National Information Technology Development Agency (NITDA) Act.³¹ Sections 17 and 18 of the NITDA Act criminalize non-

²⁷ Suit No. FHC/AB/CS/79/2020 (Unreported).

²⁸ E Chen, ‘Data Breach 2025’ <<https://www.trendmicro.com/vinfo/us/security/definition/data-breach>> accessed 13 May 2026.

²⁹ GDPR Recital 10.

³⁰ U Mokady, ‘Data Breach 2025’ <https://www.cyberark.com/what-is/data-breach/> Accessed 13 May 2026.

³¹ National Information Technology Development Agency Act 2007 (NITDA).



adherence or violation of the NITDA Act. The punishment provided for in the above stated section ranges from a fine of N200,000 or N500,000 and or one or three-years imprisonment in cases of first and subsequent offences respectively.

4.3 Fair and Lawful Processing of Personal Data

Whenever personal data is processed, it is the processor's responsibility to ensure that this is undertaken in a fair and lawful manner. 'Lawful' relates to the method of obtaining that specific data. It is going to be evident that where data has been stolen, or obtained by duress, bribes or inducements, then this is going to have been collected in an unlawful manner. 'Fair' relates to how that data is processed once it has been obtained.³² The processing of personal data should be adequate, relevant and limited to necessity of the purpose for which it is being processed, and where appropriate, with the knowledge or consent of the data subject. This principle is key to addressing practices such as the selling and or transfer of personal data that is fraudulently obtained.³³

For processing of personal data to be lawful, you need to identify specific grounds for the processing. This is called a 'lawful basis for processing, and there are six options which depend on your purpose and your relationship with the worker. If no lawful basis applies then your processing will be unlawful and in breach of this principle. Lawfulness also means that you do not do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful.³⁴

Processing of personal data must always be fair as well as lawful. If any aspect of your processing is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing. In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should. Assessing whether you are processing information fairly depends partly on how you obtain it. If anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.³⁵

To assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and workerly. If you have obtained

³² M B Abdulazeez, 'The Principles of Data Privacy and Data Protection in Nigeria' <https://www.mondaq.com/nigeria/data-protection/1177584/the-principles-of-data-privacy-and-data-protection-in-nigeria#_ftn3> accessed 8 June 2025.

³³ Ibid.

³⁴ G G Fuster, 'The Emergence of Personal Data as a Fundamental Right of the EU' [2015] *Common Market Law Review*, 4.

³⁵ D Chika and E Tochukwu, 'An Analysis of Data Protection and Compliance in Nigeria' [2020] (4) (5) *International Journal of Research and Innovation in Social Science*, 377 - 382.



and used the information fairly in relation to most of the people it relates to but unfairly in relation to one worker, there will still be a breach of this principle.³⁶

The NDPR,³⁷ provides in Part 2 Para 2.2 that without prejudice to the principles set out in this Regulation, processing shall be lawful if at least one of the following applies: the data subject has given consent to the processing of his or her Personal Data for one or more specific purposes;³⁸ and processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.³⁹ Others are processing is necessary for compliance with a legal obligation to which the Controller is subject;⁴⁰ processing is necessary in order to protect the vital interests of the Data Subject or of another natural worker,⁴¹ and processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the controller.⁴²

4.4 Consent of Data Subject

A data subject's consent is arguably the most integral requirement to obtain and process data. To lawfully do this, data controllers and processors must first seek the consent of the data subject without undue influence, fraud, and coercion.⁴³ Usually, consent is obtained through clear, unambiguous data privacy policies to which the data subject has consented. Consent should be clearly given as implied consent is no consent. Furthermore, these data are obtained subject to certain rights granted to the data subject. Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her. Consent may be made through a written statement, sign or an affirmative action signifying agreement to the processing of personal data.⁴⁴

The NDPR prescribe the circumstances under which consent may be extracted from a Data Subject as follows:⁴⁵ The specific purpose of collection of Personal Data must be made known to the Data Subject before his consent may be secured and deemed lawful; The Data Controller is obliged under the law to ensure that consent of the Data Subject is obtained without fraud, coercion or undue

³⁶ GDPR, s 1.1.17.

³⁷ NDPR, art 2 (2.2).

³⁸ NDPR, art 2 (2.2)(a).

³⁹ NDPR, art 2 (2.2)(b).

⁴⁰ NDPR, art 2 (2.2)(c).

⁴¹ NDPR, art 2 (2.2)(d).

⁴² NDPR, art 2 (2.2)(e); D Nnam, 'Informational Privacy and Security Amid Growing Activities on Electronic Platforms in Nigeria: A Case for Data Protection Law' [2019] *NAUJILJ*, 27 - 33

⁴³ NDPR, arts 2.2 and 2.3.

⁴⁴ NDPR Implementation Framework 2020.

⁴⁵ NDPR (2.3) (1) & (2).



influence; and in doing so, regard must be had to the legal capacity of the Data Subject, whether the Personal Data consented to be unambiguous.⁴⁶

The Data Subject must be aware of his right to withdraw his consent at any time (provided that he is bound by acts carried out pursuant to initial consent before withdrawal), and also, the nature of the consent must be examined, to determine whether it is conditional or excessive for the performance of the contract, and whether data is transferable to a third party under a contract. Regrettably, in Nigeria, both government agencies and private firms have consistently failed to comply with these regulations by their actions, thus costing many untold embarrassment and hardships to workers and even corporate bodies. In Nigeria, even without your knowledge, data and information about you is being generated and captured by companies and agencies that you are likely to have never knowingly interacted with.⁴⁷

4.5 Data Protection Audit

Data protection audit is a systematic investigation or examination of the records, processes and procedures of Data Controllers and Processors, to ensure that they are in compliance with the requirements of the law and their data protection policies. A data protection audit is a means of assessing whether an organisation is complying with their data protection obligations, identifying data protection risks and putting forward recommendations for best practice. The NDPR mandates all Data Controllers to conduct an audit on the data privacy policies of their organisation. The Regulations reserves the requirement for submitting data audit reports to certain categories of Data Controllers. Accordingly, only Data Controllers that process personal data of more than 1000 Data Subjects within a period of six months are mandated to file a soft copy of the summary of their audit to the NITDA. Similarly, Data Controllers that process personal data of more than 2000 Data Subjects within a period of 12 months are mandated to file a summary of their audit to NITDA, not later than 15 March in the following year.⁴⁸

Audits are meant to show that the data controller or processor complies with the law. The audit should state. The data the organisation collects on its employees and members of the public, the purpose for which such data is collected, notice given to workers regarding the collection and use of their personal information, the access given to workers to review, amend, correct, supplement, or delete such data, whether or not the consent of these workers was obtained before collecting, using, transferring, or disclosing these data; and the methods employed to obtain consent, the

⁴⁶ A Adewumi, "Adequate protection": An Analysis of Nigeria's Data Protection Laws within an Emerging Global Data Protection Framework' (an Unpublished LLM dissertation submitted at the University of Victoria in 2025).

⁴⁷ A Adeyoju, 'A Quick Guide on the Data Protection Regime in Nigeria' <https://ilca.africa/wp-content/uploads/2020/05/ADEMOLA_ADEYOJU-A-Quick-Guide-on-the-Data-Protection-Regime-in-Nigeria_compressed.pdf> accessed 6 May 2025.

⁴⁸ P Ajogbor and O. Isiadinso, 'Nigeria: Data Privacy Regulations Under The Nigerian Data Protection <Regulation 2019>' <<https://www.mondaq.com/nigeria/privacy-protection/834202/data-privacy-regulations-under-the-nigerian-data-protection-regulation-2019>> accessed 8 June 2025.



policies and practices of the organisation for the proper use and security of these data, organisation policies and procedures for privacy and data protection and the policies and procedures of the organisation for assessing the impact of technologies on the stated privacy and security policies.⁴⁹

Without a doubt, the GDPR served as a model for the NDPR when it chose data protection audit as a regulatory task. While an audit is only required once every year as part of investigatory efforts under European regulation, under the NDPR it is a required activity every year as a regulatory compliance indicator for data controllers. In order to identify any gaps that would be filled during a post-audit implementation exercise, each data controller within a specified threshold of data processing activities is expected to submit an audit summary showing its data processing activities.⁵⁰

4.6 Compensation Penalties and fines

Data breaches are every organisation's worst nightmare. They involve the breach of security of personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.⁵¹ They do not only result in the loss of the goodwill of an organisation garnered over the years, but they could also have severe financial implications capable of crippling the organisation. Regrettably, no matter how protected and prepared an organisation is against a data breach, there may still be a slim possibility of the occurrence of a breach, especially in this digital age with the proliferation of new technologies.

In Nigeria, data controllers are obligated to self-report personal data breaches to the National Information Technology Development Agency (NITDA) within 72 hours of becoming aware of such breach.⁵² This timeline is required to be documented in an organisation's data protection and privacy policy.⁵³ NDPR gave the Data Subjects the right to seek redress in Court, it also provides vide Article 4.3. (6),⁵⁴ that a breach of the NDPR is a breach of the provisions of the NITDA.

The Courts in Nigeria have on several occasions awarded damages to parties for breach of their personal data rights *Eneye v MTN Nigeria Communication Ltd*,⁵⁵ and *Anene v Airtel Nigeria Ltd*.⁵⁶ In the former case, the court held that the unauthorised disclosure of the claimant's mobile phone number by his telecommunications service provider (the defendant) and subsequent unsolicited text messages he received from unknown third parties were violations of his

⁴⁹ O Olanipekun, 'The Extent of the Right to Privacy & Data Protection in Nigeria' Esher and Makarios Law, 1<<https://esherandmakarioslaw.com/assets/resources/d1de87b4d97b68c5d88843fe2bdcf937.pdf>> accessed 6 May 2025.

⁵⁰ D Oturu, 'An Overview of big Data and Data Protection in Nigeria' (2019) *Alex*, 1.

⁵¹ NDPR art. 1.3(xxii).

⁵² NDPR, 3.2(ix) and 9.2.

⁵³ *Ibid*.

⁵⁴ *Ibid*.

⁵⁵ Appeal No: CA/A/689/2013 (Unreported).

⁵⁶ Suit No: FCT/HC/CV/545/2015 (Unreported).



constitutional right to privacy. A similar verdict was given in the latter case. Both claimants were awarded damages of N5,000,000 (five million naira), respectively.

The National Information Technology Development Agency is empowered under the Nigerian Data Protection Regulation to impose fines for any data breach by data controllers or processors. In addition to any possible criminal liability, the NDPR provides sanctions for breach of data privacy rights. Where the breach is by a Data Controller dealing with over 10,000 Data Subjects, the penalty would be 2 percent of the Data Controller's Annual Gross Revenue for the preceding year or 10 million Naira, whichever is greater.⁵⁷ For a Data Controller dealing with less than 10,000 Data Subjects, the applicable fine would be one percent of the Data Controller's Annual Gross Revenue for the preceding year or N2 million Naira, whichever is greater.⁵⁸

5. PRINCIPLES AND LAWFUL BASIS FOR THE PROTECTION AND PROCESSING OF DATA OF WORKERS UNDER THE NIGERIAN DATA PROTECTION ACT 2023

As employees are required to provide their personal information to employers for payroll, pension administration, medical benefits, and workplace monitoring, the lawful basis for collecting and processing such data is critical to ensuring that their constitutional right to privacy under section 37 of the 1999 Constitution is respected.⁵⁹ The NDPA thus operates as a safeguard against arbitrary and intrusive processing by employers, requiring that all data processing must align with the principles of lawfulness, fairness, accountability, and transparency.

Section 24 of the NDPA sets out the lawful bases for processing personal data. For Nigerian workers, the most relevant grounds include the necessity of processing for the performance of a contract of employment, compliance with a legal obligation, protection of vital interests, consent, and the pursuit of legitimate interests.⁶⁰ For instance, an employer may lawfully process an employee's bank details to pay salaries, or medical information to comply with workplace health and safety regulations. However, processing for purposes beyond these grounds, such as sharing employee data with third-party marketers, would not meet the requirements of lawfulness unless informed consent is obtained.⁶¹

The principle of consent under section 26 is particularly significant in the employment context, though it is often problematic due to the inherent imbalance of power between employer and employee. Consent must be freely given, specific, and informed. Nigerian courts, though yet to pronounce directly on NDPA provisions, have previously recognized the importance of consent in data privacy. In *Eneye v MTN Nigeria Ltd*, the Court of Appeal held that unsolicited disclosure of

⁵⁷ NDPR art 2.10(a).

⁵⁸ NDPR art 2.10(b).

⁵⁹ I P Onyeonoru, 'Labour Market in the Context of Economics Sociology: Bringing Society back to the Economy' (2008) (6)(1) *Ibad. J. Soc. Sc.*, 55-67.

⁶⁰ M K Idowu, 'Job Satisfaction among Contract Workers in Intercontinental and First Banks in Ibadan' (2010) (2)(4) *Journal of Dept of Soc., Uni. Of Ibadan, Nigeria*, 321.

⁶¹ N Anyasi, 'Privacy of Electronic Communications in Work Place' [2025] (11)(2) *Nigerian Bar Journal*, 183.



subscriber data without consent amounted to a violation of the right to privacy under section 37 of the Constitution. Applying the same reasoning, an employer who processes or discloses employee data without valid consent risks liability under the NDPA, particularly where such processing cannot be justified under contractual or statutory grounds.⁶²

Another key lawful basis under section 24 is legitimate interest. This permits employers to process worker's data where such processing is necessary for organizational efficiency, provided it does not override the rights and freedoms of employees. The jurisprudence of the European Court of Human Rights in *Bărbulescu v Romania* is instructive in this regard. In that case, workplace surveillance was scrutinized against the right to privacy, and the Court stressed the need for proportionality and prior notification to the employee.⁶³

5.1 Nexus between Legitimacy of Interests and Privacy Rights of Workers under the Nigerian Data Protection Act 2023

In practice, legitimate interest is broad enough to cover employer activities such as monitoring email communications, CCTV surveillance, and vetting employees for security purposes. Yet, section 24(2) of the NDPA requires that such processing be proportionate, necessary, and not override the rights and freedoms of the data subject.⁶⁴ The European Court of Human Rights decision in *Bărbulescu v Romania* illustrates this balance, where surveillance of an employee's communications was held unlawful because it failed to adequately protect his privacy rights. Nigerian courts, though yet to directly apply the NDPA, may draw guidance from such jurisprudence in determining when employer reliance on legitimate interest crosses into unlawful intrusion.⁶⁵

Nigerian case law already affirms the centrality of privacy in the workplace. In *Eneye v MTN Nigeria Ltd*, the Court of Appeal held that unauthorized disclosure of subscriber data violated section 37 of the Constitution. Similarly, in *Anene v Airtel Nigeria Ltd*,⁶⁶ damages were awarded for unsolicited messages that breached privacy. These cases, though predating the NDPA, demonstrate a judicial willingness to uphold privacy against corporate practices. The nexus between legitimate interests and worker privacy under the NDPA thus rests on a balancing test. Employers must demonstrate that the processing of worker data serves a genuine interest essential to business operations, while employees retain the right to challenge processing that infringes disproportionately on their privacy.⁶⁷ Section 33 of the NDPA strengthens this position by granting

⁶² Anyasi (n 61).

⁶³ Ibid.

⁶⁴ Lilies and Others, *A Survey of the Legal Issues Facing Digital Forensic Experts* (Springer 2009) 123.

⁶⁵ Ibid.

⁶⁶ *Ezugwu Emmanuel Anene v Airtel Nig. Ltd* Suit No. FCT/HC/CV/545/2015 (Unreported).

⁶⁷ A Elgujja, 'A Synopsis on Data Protection under the Nigerian Laws: Has the Universality of Right to Privacy Trickled Down to Nigeria?'

<<https://usir.salford.ac.uk/60203/1/Data%20Protection%20under%20the%20Nigerian%20%20Laws%20Final%20%281%29.pdf>> accessed 6 May 2026.



workers the right to object to certain forms of processing, thereby ensuring that legitimate interest does not become a blanket justification for data misuse.

6 CHALLENGES IN THE ENFORCEMENT OF THE RIGHT TO PRIVACY OF THE NIGERIAN WORKERS

In Nigeria, the expansion of data privacy has been stifled for several reasons, notable among which are:

6.1 Inappropriate/Inadequacy of Data Privacy Legislation

There is no denying that the NDPA is a noteworthy government endeavor designed to fill the gap left by Nigeria's lack of a legislative framework for data protection before its passage in 2019. The NDPR was designed as a stopgap solution, nevertheless, to lay the groundwork for the adoption of a full and meaningful data protection law in Nigeria. This helps to explain some of the NDPR's flaws and gaps, which have seriously limited Nigeria's ability to comply with data protection laws.⁶⁸ Lack of an extraterritorial scope in the legislation, which might have addressed concerns relating to cloud storage of personal data gathered from Nigeria on servers located in other countries, Lack of any requirement for data controllers to maintain track of processing operations, lack of any requirement to appoint a legal representative in Nigeria for data controllers who process personal data collected from the nation, among other things. This helps to explain why there isn't much legal precedent in Nigeria for data protection.⁶⁹

Just like every other developing nation, inappropriate legislation to data protection has hampered data protection and compliance in Nigeria. Nigeria laws on data protection and privacy are not specific to the target. Not until January 25, 2019, Nigeria did not have any devoted general enactment on data privacy and protection apart from the 1999 Constitution which has not been particularly useful for the purpose of data privacy especially given the fast pace of technological advancements and the associated complexities and also considering our courts somewhat restrictive approach to the interpretation of the relevant section on privacy.⁷⁰

In spite of the fact that the provision above does not explicitly make reference to “data,” it is arguable that information on homes, correspondences and telephone conversations is captured in the definition of personal data; hence, the above provision can be utilized to defend such breach. In addition, these inadequacies are manifested in the lack of an analogy between data breaches and their conventional counterparts. For instance, trespassing and hacking into a computer network.

⁶⁸ Luminate, 'Data & Digital Rights in Nigeria Assessing the activities, issues and opportunities' A Stears Data Report of 2025.

⁶⁹ O Alao, 'The Nigeria Data Protection Bureau and the Challenges Of Data Privacy Compliance In Nigeria' <<https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-data-protection-bureau-and-the-challenges-of-data-privacy-compliance-in-nigeria>> accessed 8 June 2025.

⁷⁰ For instance, CFRN 1999, s 37; A Elgujja, 'A Synopsis on Data Protection under the Nigerian Laws: Has the Universality of Right to Privacy Trickled Down to Nigeria?' <<https://usir.salford.ac.uk/60203/1/Data%20Protection%20under%20the%20Nigerian%20Laws%20Final%20%281%29.pdf>> accessed 6 May 2025.



The penalty on trespass does not hold against hacking and accessing private data. This clearly illustrates a challenging situation whereby no relevant laws on hacking are available. Therefore, there are a lot of inadequacies in the Nigeria legislation on data protection which is also expected to be the case in other developing countries⁷¹.

Again, even with the emergence of NDPR the capacity to adequately protect personal data and privacy especially in respect to data collection, control and processing fall short of international standard. For instance, the NDPR has been criticized for being sketchy compared to its European equivalent, the General Data Protection Regulations. Although comparison, uncovers that the NDPR borrows a lot from the GDPR in its fundamental principles, it takes the issue of data privacy as a fundamental right of the data owner (or data subject) which should be protected through regulatory oversight even though the data has been submitted to a company for the provision of services. Therefore, the lack of uniformity in data control is also a major challenge as it uncovered workers and businesses to various entry points. Be that as it may, the existence of many buckets of data is not exclusive to Nigeria. The difference is that, whereas the countries in the western world have attained a certain level of maturity in the handling of buckets of data, Nigeria is still on the way.⁷²

6.2 Reporting Data Breaches

Most data breaches continue to go unreported to the data subjects or undocumented, despite the development of NDPR in Nigeria. This has been ascribed to a number of factors, including delays in notifying data subjects of breaches in some circumstances, reporting data breaches to the authority and the authority's requirement to inform the data controller whether to notify the data subject of the breach. This is in violation of Article 33 of the GDPR, which requires controllers and processors to notify the supervisory authority and affected parties of data breaches within 72 hours if they constitute a risk to implementation. As a result, African data protection and privacy legislation will need to implement suitable reporting systems in the event of data breaches.⁷³

Olumide⁷⁴ noted that data protection and privacy are essentially alien concepts to Nigerian society as evidence for this. The majority of data subjects are uninformed of their property rights in their data, and the majority of data collectors and administrators are unaware of their need to secure and/or respect the privacy of the data entrusted to them. Finally, a startling complicit stillness or absence of controllers in this field appears to have existed. Nigerians have never genuinely cared about what happens to their information as long as their other financial/physical rights remained

⁷¹ D T Muli and N M Mutua, 'Addressing the Challenges of Data Protection in Developing Countries' [2013] 1(1) *European Journal of Computer Science and Information Technology*, 1- 9.

⁷² O Babalola, 'Data Protection and Privacy Challenges in Nigeria (Legal Issues)' <<https://sig.ng/wp-content/uploads/2019/07/DATA-PROTECTION-AND-PRIVACY-CHALLENGES-IN-NIGERIA.pdf>> <accessed 6 May 2025>.

⁷³ N Aderibigbe, 'Data Protection in Nigeria: What Organizations Need to Know' <www.jacksonettiaandedu.com> accessed 6 May 2025.

⁷⁴ O Babalola, 'Data Protection and Privacy Challenges in Nigeria (Legal Issues)' accessed 9 June 2025.



unaffected, but that has changed in recent years with the development of a tiny number of civil societies that have made data privacy and protection their top priorities. Therefore, analysts highlight that in a nation where people's personal data are shared without their agreement compliance might be difficult for many organisations, especially government agencies.⁷⁵

6.3 Consent to Data Collection

The consent for one's personal data, which is a crucial component of Nigerian data privacy, is another crucial issue. Safeguarding laws and international data protection laws in particular. Consent means that in order to be legitimate, obtained before the data collection, particularly through the aim of data gathering is clearly stated, and a statement that further consent is required where it is personal data may be disclosed to outside parties. Moreover, those facts Controller obtains and records worker consent, additionally, a clause allowing for the withdrawal of consent whenever they choose.⁷⁶ Regrettably, both public and private organizations in Nigeria have repeatedly disobeyed these laws by their conduct, causing immeasurable suffering and shame to people and even corporate entities. In Nigeria, businesses, and organizations that you are likely to never have intentionally interacted with are generating and capturing data and information about you without your awareness.

6.4 Lack of Enforcement

In addition to the country's insufficient data privacy laws, numerous social critics and scientists have highlighted worries about the capacity of Government to follow the guidelines in the information protection regulation because several parastatals and agencies were recognised for breaking the law. Therefore, despite developing the NDPR statute by NITDA, it shouldn't stop there. The various Data Collectors have not disclosed their privacy rules, nor did NITDA sanction them as required by section 2.10 of the NDPR, giving rise to the rebuttable perception that the authorities are treating them with kid gloves.⁷⁷

There are other regulations that must be followed immediately and consistently, such as section 4.3(2), which calls for each Data Controller to appoint a Data Protection Officer. This requirement is tragically non-existent and is still not being implemented by the regulator. One instance that immediately comes to mind is the Nigeria Immigration Service's recent violation of the NDPR as a result of the publishing of the international passport data page of a Nigerian resident of the UK. Without the data subject's consent, the information was posted on the Service's social media platforms. However, it appears that the Immigration Service has not received any disciplinary action under the NDPR.⁷⁸ There are more websites run by the Nigerian government that have

⁷⁵ A Adegoke, 'Data Rights and Privacy in Nigeria' A report published by The Paradigm Initiative in 2020.

⁷⁶ European Data Protection Board (2016) Guidelines on Consent under Regulation 2016/679 (WP259, rev.01) <www.europeandataprotection.com/pdf> accessed 8 June 2025.

⁷⁷ T Adedola, and others, 'Nigerians' Perceptions of Personal Data Protection and Privacy' <<https://www.researchgate.net/publication/275968129>> accessed 6 May 2026.

⁷⁸ (n 30).



similar weaknesses. By entering the name and CAC registration number somewhere on the CAC website, you may learn everything there is to know about a company, including the directors' names, addresses, phone numbers, and other information. Given that the majority of businesses have their CAC number in their emblem, this is shocking. Many other websites can be readily tricked to obtain extremely private information about people.⁷⁹

6.5 Dearth of Practicing Professionals

It is important to note that, even as Nigeria improves, there is still a long way to go. In an effort to stay current, many businesses are going digital in order to reach a wider audience and establish themselves in the global marketplace. Is adopting digital technology and using digital systems more than just a fashion statement? And if cybersecurity is given enough consideration, it can involve hiring the appropriate staff to supervise company information systems and ingraining data privacy into the corporate culture. Regrettably, numerous incidents have demonstrated Nigeria's businesses propensity to misuse their consumers' personal data, particularly in the telecommunications sector⁸⁰ and occasionally to sell these data to outside parties. Even among worker data consumers, the vast majority are unaware of the idea of sensitive information and how it might be traded online. The Global Data Protection Regulation (GDPR), which is anticipated to change the hierarchical structure of both the private and public sectors, as well as keeping up with the law and technological updates that are constantly in motion regarding data privacy and protection, are other pertinent challenges that probably data privacy and compliance in Nigeria must contend with. Of course, this called for the use of knowledge and experts, including specialists like Data Protection Officers (DPOs). Nigerians and people in many other third-world countries are familiar with this function, in contrast to many western countries, yet there aren't many working professionals there.⁸¹

In addition, many Nigerian businesses, despite everything, view the NDPR hype with a degree of skepticism and covertly wish it would go away due to the time and resources required for compliance. Fortunately, the existence of data privacy regulations is increasingly seen as a sign of trust in a country's online commercial environment. Data protection is becoming a risk concern that is handled at the negotiation stage between companies in different countries as organisations grow more globally connected and information trade becomes an indispensably crucial component of business exchanges. Data privacy must be taken seriously by nations that want to develop public confidence in the infrastructure they have in place for online commerce.⁸²

⁷⁹ M D Chika and I S Tochukwu, 'An Analysis of Data Protection and Compliance in Nigeria' (2020) (4)(5) *International Journal of Research and Innovation in Social Science (IJRISS)*, 2454-6186.

⁸⁰ F Eleanya, 'The NDPR Isn't Perfect but It's a Step to Data Protection for Nigeria. Business Day' <<https://businessday.ng/technology/article/the-ndpr-isnt-perfect-but-its-a-step-to-data-protection-for-nigeria>> accessed 9 June 2025.

⁸¹ A Dode, 'The challenges of implementing General Data Protection Law (GDPR)'" <https://www.academia.edu/37461999/The_challenges_of_implementing_General_Data_Protection_Law_GDPR_> accessed 10 June 2025.

⁸² Ibid.



7. CONCLUSION

The NDPA constitutes a significant advancement in the protection of personal data in Nigeria. It elevates privacy safeguards to a statutory level and aligning the country more closely with international best practices. In the employment sphere, its principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and security (Section 24) provide a solid foundation for protecting workers' rights against arbitrary or excessive data processing. The explicit recognition of legitimate interest as a lawful basis (Section 25), the tailored rules for sensitive personal data in employment and social security contexts (Section 30(1)(b)), and the comprehensive catalogue of data subject rights including access, rectification, erasure (notably upon termination of employment), objection, and withdrawal of consent empower employees as active participants in the governance of their personal data. Nevertheless, the appraisal reveals that the NDPA, while ambitious, falls short of fully addressing the unique dynamics of the workplace. The absence of sector-specific provisions on electronic monitoring, biometric systems, or automated HR decisions leaves employers and workers without clear guidance, risking inconsistent application and potential rights violations. The practical limitations of consent in hierarchical employment relationships, coupled with enforcement capacity constraints at the NDPC and the nascent state of implementing regulations, further temper the Act's transformative potential. Overall, the NDPA marks a commendable but incomplete step toward robust protection of workers' data rights. Its ultimate success will depend on proactive regulatory elaboration and stakeholder engagement.

8. RECOMMENDATIONS

To maximise the NDPA's protective impact on workers' rights, the following recommendations are proposed:

1. **Regulatory Guidance from the NDPC:** The Commission should urgently issue sector-specific guidelines or a Code of Conduct for workplace data processing, covering employee monitoring (CCTV, email surveillance, GPS), biometric attendance, DPIA templates for HR systems, and legitimate interest assessments tailored to employment contexts. These should clarify when consent is inappropriate due to power imbalances and mandate transparent privacy notices and policies.
2. **Legislative or Subsidiary Amendments:** Consider targeted amendments or regulations to expressly regulate workplace surveillance, introduce collective rights for trade unions (for example, consultation on monitoring policies), and operationalise data portability. Alignment with existing labour statutes (Labour Act, Employee Compensation Act, etc.) should be harmonised to avoid conflicts.
3. **Employer Best Practices:** Organisations should appoint Data Protection Officers (where required under Section 32), conduct regular DPIAs for high-risk processing, implement privacy-by-design in HR technologies, and provide mandatory data protection training to



HR and management staff. Retention policies must strictly adhere to the storage limitation principle, with automatic deletion protocols post-employment were lawful.

4. **Capacity Building and Awareness:** The NDPC, in collaboration with the Ministry of Labour and Employment and civil society, should launch nationwide awareness campaigns and training programmes for workers and unions on exercising data subject rights. Legal aid mechanisms for data breach complaints should be strengthened.
5. **Enforcement and Research:** The NDPC should prioritise proactive audits of major employers and publish annual enforcement reports. Academic and policy research on the NDPA's real-world impact in the workplace should be encouraged to inform iterative improvements.