Data Privacy and Protection
8th November 2024



Ibukun Spaine[1]

APPLICABLE LAWS IMPACTING PRIVACY AND DATA PROTECTION UNDER NIGERIAN LAW

INTRODUCTION

The legal landscape in Nigeria pertaining to data privacy and protection is dynamic and ever-changing, influenced by a blend of sector specific regulations, recent laws, and constitutional provisions. The Constitution, which protects citizens' rights to privacy of their homes, correspondence, telephone communications, and telegraphic communications, is the cornerstone of Nigeria's data privacy laws. The country's data protection laws are firmly based on this fundamental principle. The Constitution does not, however, cater for how this right should be applied or upheld in the digital era. The Nigerian Data Protection Act (NDPA) was passed into law in 2023 in response to the expanding demand for thorough privacy and data protection practices.

The NDPA represents a significant advancement in governing the handling of personal data in Nigeria. This article explores the relevant laws affecting privacy and data protection within the Nigerian legal framework.

LAWS IMPACTING PRIVACY AND DATA PROTECTION UNDER NIGERIAN LAW

1. **The 1999 Constitution of the Federal Republic of Nigeria (as amended)**

   Section 37 of the Constitution of the Federal Republic of Nigeria (CFRN) 1999 (as amended) guarantees the right to privacy. This is the foundation of Data Privacy

[1] **Ibukun Spaine,** Dispute Resolution Department, Graduate Intern, S.P.A. Ajibade & Co., Lagos, Nigeria.

Protection as a constitutionally assured right in the country as set out in the fourth chapter. Section 37 of the CFRN provides that:

> *The privacy of citizens, their homes, correspondence, telephone communications and telegraphic communications is hereby guaranteed and protected*.[2]

This provision by virtue of the authority imbued in the Constitution extends the right of privacy to all individuals to cover their homes, their personal conversations, their communications by way of telephone or by telegraph. One commentator has expatiated on the ramifications of section 37 of the Constitution as encompassing the privacy of the person (i.e. from unwanted incursions into physical, emotional and personal attributes); the sanctity of homes and property (i.e. from unauthorized searches and trespasses); and the protection of correspondence and conversations from being intercepted and diverted.[3]

2. Nigeria Data Protection Act

The Nigeria Data Protection Act, 2023 ("NDPA") was signed into law by President Bola Ahmed Tinubu on the 14th of June, 2023.[4] The NDPA 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.[5] The NDPA, which was enacted by the National Assembly, applies to the processing of personal data within Nigeria, including the processing of personal data of a Nigerian data subject by data controllers and processors resident or domiciled abroad.[6] There is a legal requirement under this law to report a breach of its provisions to the data protection authority.

Section 40 of the NDPA provides that a Data Controller or Processor is expected to report any incidence of a breach to the NDPC within 72 hours of becoming aware of

---

2 Section 37 of the Constitution of Federal Republic of Nigeria, 1999 (as amended).

3 Adedeji Adekunle, 'Right to Privacy and Law Enforcement' being the Text of a Lecture presented at the Ogun Judges Conference (2016) available at <https://nials.edu.ng/pdf/RIGHT%20TO%20PRIVACY%20AND%20LAW%20ENFORCEMENT%20JSC%20PRESENTATION%20%20(PROF%20%20ADEKUNLE).pdff> accessed 30 September 2024.

4 Peter and Ndinojuo, 'Privacy Awareness and Social Media: Personal Data Protection among Facebook and Instagram Users' (2024) available at <https://galacticamedia.com/index.php/gmd/article/view/489/443#:~:text=The%20principal%20data%20protection%20legislation%20in%20Nigeria%20is%20the%20Nigeria,Nigeria%201999%20(as%20amended)> accessed 30 September 2024.

5 Ibid.

6 Section 2 of the Nigeria Data Protection Act, 2023.

the breach. This timeline is required to be documented in the organization's data protection policy and privacy policy. The details to be reported include:

a. A description of the nature of the Personal Data breach including the categories and approximate number of Data Subjects and Personal Data records concerned.

b. The name and contact details of a point of contact of the Data Controller, where more information can be obtained.

c. A description of the likely consequences of the Personal Data breach.

d. A description of the measures taken or proposed to be taken to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

e. A description of steps the organization has taken to reduce the risk of harm to individuals.[7]

3. Cybercrime (Prohibition, Prevention) Amendment Act (2024)

This is a federal legislation passed into law in 2015 to answer the fervent clamor of a need for legislation to curb internet fraud and cybercrimes.[8] While it is apparent that this Act is not in direct correlation with the need for Data Privacy, one of the objectives of the Act is to promote cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights as contained in Section 1(c) of the Act.[9] The Cybercrime Act is a comprehensive legislation aimed at combating cybercrime and protecting Nigeria's digital space. Sections 16,[10] 22,[11] 29,[12] and 38[13] of the Act specifically address data protection and privacy.

4. The Central Bank of Nigeria Consumer Protection Framework, 2016

---

7 Section 40 of the Nigeria Data Protection Act, 2023.

8 Modesta Egiyi, 'The Adoption of Advanced Cyber Laws as an Effort to Curb Internet Fraud in Nigeria' (2020) available at <https://www.researchgate.net/publication/350670907_The_Adoption_of_Advanced_Cyber_Laws_as_an_Effort_to_Curb_Internet_Fraud_in_Nigeria> accessed 30 September 2024.

9 Section 1(c) of the Cybercrimes (Prohibition, Prevention) Act, 2015.

10 Section 16 of the Act prohibits unauthorized modification of computer data, imposing fines and imprisonment for offenders.

11 Section 22 of the Act addresses identity theft, impersonation, and fraudulent use of electronic signatures, with penalties including imprisonment and fines.

12 Section 29 of the Act holds service providers liable for fraudulent activities, including forging security codes, with fines and potential winding up of corporate offenders.

13 Section 38 of the Act mandates service providers to retain traffic data and subscriber information for two years, release information to law enforcement agencies, and safeguard confidentiality.

The Central Bank of Nigeria (CBN) Consumer Protection Framework (the Framework) was issued by the CBN by virtue of the power invested in it according to Section 51 of the CBN Act of 2007 (as amended) and Section 55 of the Banks and Other Financial Institutions Act 2007 (BOFIA).[14] The purpose of this Framework is to provide guidance in the effective regulation of consumer protection with nine key principles.[15] Of these nine key principles, it can be observed that the sixth principle concerns the subject of Data Privacy and Protection. Regulation 2.6 of the Framework stipulates that:

> *Appropriate measures shall be established to guarantee protection of consumer assets and privacy. Consumer's financial and personal information shall be always protected by Financial Institutions and shall not be released to third party without the consent of the consumer, except as required by law.*[16]

Regulation 2.6 of the Framework provides that information that may be considered sensitive such as account numbers, contact details, statement of accounts, account balance and the like known to Financial Institutions are considered confidential and must be protected always.

5. The National Information Technology Development Agency Data Protection Regulation

The Nigeria Data Protection Regulation (hereinafter referred to as NDPR) was issued in the year 2019 pursuant to the mandate given to the National Information Technology Development Agency (hereinafter referred to as NITDA) in Section 6(c) of the NITDA Act.[17] This section compels the NITDA to develop guidelines and regulations for electronic governance and to monitor the use of electronic data interchange and other forms of electronic communication transactions. Part Two of the NDPR which contains the NDPR's manifestation of the Fair Information Principles (illustrates the NDPR's position on data privacy and protection and is partly captured in Article 2.3 of the NDPR. That provision regulates the method by which consent is procured and the manner in which information is to be processed and stored.[18]

6. Freedom of Information Act

---

14 Section 55 of the Banks and Other Financial Institutions Act, 2007.

15 Islamic Market, 'Consumer Protection Framework' available at <https://islamicmarkets.com/publications/consumer-protection-framework-by-central-bank-of-nigeria>accessed 30 September 2024.

16 Regulation 2.6 of the Central Bank of Nigeria Consumer Protection Framework, 2016.

17 Section 6(c) of the National Information Technology Development Agency, 2001.

18 Article 2.3 of the Nigeria Data Protection Regulation, 2019.

With the rise of the democratic system in Nigeria and after years of military regimes, there came a clear call from the people for there to be more transparency in the actions of the government in carrying out its activities. A result of this clamor is the Freedom of Information Act (FOIA). This Act gives public institutions the power to deny any request for information that contains personal information.[19]The FOIA grants the public access to public records and information as an effort to lift the shroud of obscurity on the actions of the government. This is done in a way that holds the interest of the public close and guarantees the protection of personal information and privacy. Section 14(1) of the FOIA provides that 'a public institution must deny an application for information that contains personal information.' With this provision it is clear that the FOIA cannot be used to gain access to information that is seen as sensitive or personal. This Act defines what may constitute personal information as "any official information held about an identifiable person but does not include information that bears on the public duties of employees and officials.[20] The Freedom of Information Act (FOIA) in Nigeria strikes a balance between transparency and data privacy. While granting public access to records, it safeguards personal information. Section 14(1) mandates institutions to deny requests containing personal data, ensuring sensitive information remains protected. The Act defines personal information as data about identifiable individuals, excluding information related to public duties. This provision shields citizens' privacy while promoting government accountability. By limiting access to sensitive information, the FOIA prevents potential misuse and maintains trust in government institutions. This balance fosters openness while respecting individuals' right to privacy.

7. The Credit Reporting Act, 2017

This act was promulgated with the aim of helping small and medium businesses access the opportunity of accessing credit loan facilities with the aid of movable assets as a means of security to get loans from financiers[21]. To achieve this objective, the Credit Reporting Act (CRA) collates 'credit information' and any related information that may be required in the process of decision making by the creditors. Credit information is defined in the CRA as:

Information bearing on a person's credit worthiness, credit standing or capacity, and to the history and profile of such person with regards to credit, assets, and any financial obligations, including such person's demographic data and such other information that

19 Section 14 of the Freedom of Information Act 2011.
20 Section 30 of the Freedom of Information Act 2011.
21 Izuchukwu Nnema, 'Collateral Registry Act, Credit Reporting Act 2017 and Nigeria's economy' (2017) available at <https://guardians.ng/features/law/collateral-registry-act-credit-reporting-act-2017-and-nigeria%E2%80%99s economy-2.> accessed 30 September 2024.

may aid credit decision making.[22] The Credit Reporting Act, 2017, balances credit accessibility with data privacy. While facilitating credit decisions, it protects individuals' sensitive information. The CRA defines “credit information” broadly, including demographic data. However, it ensures data privacy by regulating collection, storage, and disclosure, thereby safeguarding individuals' financial information and promoting trustworthy credit systems.

8. The National Information Technology Development Agency Data Protection Regulation

The Nigeria Data Protection Regulation (hereinafter referred to as NDPR) was issued in the year 2019 pursuant to the mandate given to the National Information Technology Development Agency (hereinafter referred to as NITDA) in Section 6(c) of the NITDA Act.[23] This section compels the NITDA to develop guidelines and regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions. The NDPR is the only item in the Nigerian Data Privacy protection framework whose focal point is data protection. This is evident in Part Two of the NDPR which contains the NDPR’s manifestation of the Fair Information Principles (hereinafter referred to as FIPs). To illustrate the NDPR’s position on the FIPs, an analytical gaze can be turned to Article 2.3 of the NDPR which regulates the method by which consent is procured and the manner as to which information is processed and stored.[24]

The Nigeria Data Protection Regulation (NDPR) 2019 is a groundbreaking legislation that prioritizes data protection in Nigeria. Issued by the National Information Technology Development Agency (NITDA), it establishes guidelines for electronic governance and monitors electronic communication transactions. According to Regulation 4.1(8) of the NDPR,[25] the mass media and civil societies may uphold accountability and foster the objectives of the NDPR. Section 9.1 of the NDPR Implementation Framework provides that, in addition to Data Subjects and government agencies, civil societies or professional organisations may also report a breach of the NDPR to the NDPC.[26]

9. The Nigerian Communication Commission General Consumer Code of Practice Regulations for Telecommunications Service Providers

22 Credit Reporting Act 2017 Interpretation Section.
23 Section 6(c) of National Information Technology Development Agency.
24 Article 2.3 of the Nigeria Data Protection Regulation.
25 Regulation 4.1(8) of the Nigeria Data Protection Regulation 2019.
26 Section 9.1 of the Nigeria Data Protection Regulation Implementation Framework.

The Registration of Subscribers Regulation of 2011 (RTS) emerged from the rise of SIM card registration policies in African countries to clamp down on criminal activities. Scholars believed the large amounts of unregistered SIM cards could be causally linked to crime.[27] To combat this, by virtue of Section 70 of the NCA, the NCC 2011 created the RTS to ensure there was a regulatory framework to guide the registration of SIM cards to Mobile Telephone Services. This was also for the establishment, control, administration, and management of the Central Database.[28] The Regulations apply to all persons and Licensees.

10. Nigerian Communications Commission Registration of Telephone Subscribers Regulation, 2011.

The Registration of Subscribers Regulation of 2011 (RTS) emerged from the rise of Subscriber Identity Module (SIM) card registration policies in African countries to clamp down on criminal activities. Scholars believed the large amounts of unregistered Subscriber Identity Module could be causally linked to crime.[29] To combat this, by virtue of Section 70 of the NCA, the NCC 2011 created the Registration of Subscribers Regulation to ensure there was a regulatory framework to guide the registration of SIM cards to Mobile Telephone Services. This was also for the establishment, control, administration, and management of the Central Database.[30] The Regulations apply to all persons and Licensees.

11. Child Rights Act

The Child Rights Act[31] regulates the protection of children (persons under the age of 18 years). Section 8 of the Child Right Act guarantees every child's entitlement to privacy, family life, home, correspondence, telephone conversation and telegraphic communications,[32] while section 205(2) prohibits the publication of any information that will lead to the identification of a child offender, and requires that the records of child offenders be kept strictly confidential and closed to third parties except in certain limited

---

27 Aaron OlaniyiSalau, 'Data Protection in an emerging economy; the case of Nigeria Communications Commission: Regulation without predictability?' (2016) available at <https://icil.gr/download.php?fen=years/2016/downloads/speakers/0083-salau-full_text-en-v2.pdf> accessed 30 September 2024.

28 Regulation 2 of the Registration of Subscribers Regulation.

29 Aaron OlaniyiSalau, 'Data Protection in an emerging economy; the case of Nigeria Communications Commission: Regulation without predictability? 'available at <https://icil.gr/download.php?fen=years/2016/downloads/speakers/0083-salau-full_text-en-v2.pdf> accessed 30 September 2024.

30 Regulation 2 of the Registration of Subscribers Regulation.

31 Child Rights Act 2003, available at < https://placng.org/lawsofnigeria/laws/C50.pdf> accessed 30 September 2024.

32 Section 8 of the Act.

circumstances. Following from the above mentioned principles this Act protects vulnerable children's sensitive information, promoting their well-being and safety.

12. The Credit Reporting Act, 2017

This act was promulgated with the aim of helping small and medium businesses access to the opportunity of accessing credit loan facilities with the aid of movable assets as a means of security to get loans from financiers.[33] To achieve this objective, the Credit Reporting Act (CRA) collates 'credit information' and any related information that may be required in the process of decision making by the creditors. Credit information is defined in the CRA as:

Information bearing on a person's credit worthiness, credit standing or capacity, and to the history and profile of such person with regards to credit, assets, and any financial obligations, including such person's demographic data and such other information that may aid credit decision making.[34] The Credit Reporting Act (CRA) facilitates credit access for small businesses, but raises data privacy concerns. It collects sensitive information, including demographic data, credit history, and financial obligations. The CRA must balance credit facilitation with data protection, ensuring confidentiality, accuracy, and secure storage to safeguard individuals' financial information and privacy.

13. The National Health Act

The National Health Act was enacted in 2014 as an Act to provide a framework for the regulation, development and management of a national health system and set standards for rendering health services in the Federation and for related matters.[35] Prior to the enactment of the Act, there was no federal legislation that attempted to outline the rights of patients (consumers) in the Nigerian healthcare sector, especially with regards to the duty of confidentiality owed by healthcare personnel and workers. In very clear language, the Act stipulates that healthcare workers shall give a user relevant information pertaining to his or her health and forbids the same information being disclosed to other persons except on certain conditions.[36]

---

33 Izuchukwu Nnema, 'Collateral Registry Act, Credit Reporting Act 2017 and Nigeria's economy' (2017) available at <https://guardians.ng/features/law/collateral-registry-act-credit-reporting-act-2017-and-nigeria%E2%80%99s economy-2.> accessed 30 September 2024.

34 Ibid.

35 Osahon Enabulele, 'Nigeria's National Health Act: An assessment of health professionals' knowledge and perception' (2016) *NCBI* available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5036296/> accessed 30 September 2024.

36 Ibid.

The Act makes clear provisions for the protection of personal health information in sections 26 – 29 of the Act. Section 26(1) lays down the duty of confidentiality by providing that "All information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential." This duty of confidentiality between healthcare providers and patients is an age old one. The import of the foregoing provision is that it is not only doctors that owe this duty, but everyone working in the precincts of a healthcare provider. Subsection (2) of the section goes further to state that "no person may disclose any information contemplated in subsection (1) unless –

(a) The user consents to that disclosure in writing;

(b) A court order or any law requires that disclosure;

(c) In the case of a minor, with the request of a parent or guardian;

(d) In the case of a person who is otherwise unable to grant consent upon the request of a guardian or representative; or

(e) Non-disclosure of the information represents a serious threat to public health.[37]

This is a strong codification of the duty of confidentiality that medical personnel owe the users of healthcare services. Apart from the above-mentioned six grounds, on no other account may personal health information be disclosed to someone who is not a healthcare giver or provider or working in a health establishment. In other words, except the recipient is in the line of duty, personal health information should not be disclosed to him or her.[38]

14. **Guidelines for the Management of Personal Data by Public Institutions**

The National Information Technology Development Agency (NITDA) issued the Guidelines for the Management of Personal Data by Public Institutions in Nigeria in 2020. These guidelines aim to protect Nigerian citizens' personal data when interacting with public institutions.[39] Key highlights include:

---

37 National Health Act 2014, section 26.

38 See, J. Onyido, S. Eke, F. Okoro, and M. Abdulsalam, "Data Protection and Privacy Concerns in the Management of Medical and Health Data in Nigeria" in *Emerging Jurisprudence on Privacy and Data Protection in Nigeria*, (UpThought Limited, 2023): pp 105 – 134.

39 Tolulope Ayanbola, 'Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020' (2020) available at <https://www.aluko-oyebode.com/insights/guidelines-for-the-management-of-personal-data-by-public-institutions-in-nigeria-2020/>accessed 30 September 2024.

i. Protection of Personal Data: All forms of personal data of Nigerian citizens are protected when interacting with public institutions.[40]

ii. Legitimate Interest: The guidelines provide an additional basis for lawful processing, including the legitimate interest of the data subject.

iii. Endorsement Requirement: Processing data for public, legal, or vital interest requires endorsement or signature from high-ranking officials.

iv. Prohibition on Purpose Expansion: Public institutions cannot change or expand the original purpose of data collection without statutory authority or data subject consent.[41]

These guidelines provide a framework for public officers to manage personal information in compliance with the Nigeria Data Protection Regulation 2019.

15. Official Secrets Act

The Official Secrets Act, enacted in 1962, aims to secure public safety and protect national security by restricting the disclosure of classified information.[42] However, this Act has significant implications for privacy and data protection in Nigeria.

a. Restrictions on Information Flow

The Act prohibits the transmission, obtainment, reproduction, or retention of classified matter without authorization.[43] This restriction limits the flow of information, potentially impacting transparency and accountability in governance.

b. Protection of Defence Establishments

The Act criminalizes unauthorized entry, photography, or recording of protected places, including defence establishments.[44] While national security concerns justify these measures, they may also infringe on individual rights to freedom of movement and expression.

c. Emergency Restrictions

During periods of emergency, the President can restrict photography, sketching, or recording of defence-related materials.[45] This provision may be

40 Ibid.
41 Ibid.
42 Official Secrets Act 1962, available at <https://gazettes.africa/archive/ng/1962/ng-government-gazette-supplement-dated-1962-10-20-no-84-part-a.pdf> accessed 30 September 2024.
43 Section 1 of the Act.
44 Section 2 of the Act.
45 Section 3 of the Act.

used to suppress information, potentially violating freedom of expression and press.

16. CBN Guidelines on Point of Sale Card Acceptance Services

The Central Bank of Nigeria's (CBN) Guidelines on Contactless Payment in Nigeria, issued in June 2023, aim to regulate contactless payment transactions and ensure secure and efficient financial services.[46] While the Guidelines primarily focus on security standards and transaction limits, they also have significant implications for privacy and data protection under Nigerian law. The Guidelines require stakeholders to comply with international security standards, such as ISO 14443, and Payment Scheme and Card Scheme certifications.[47] This alignment with global best practices reinforces the Nigeria Data Protection Regulation emphasis on data protection and privacy.

The Guidelines mandate merchants to store contactless payment records, data, and documents in accordance with extant laws and regulations, including the Nigeria Data Protection Act (NDPA) 2023. This ensures that personal data is retained only for necessary purposes and disposed of securely. The Guidelines require immediate reporting of security incidents to the CBN within 24 hours.[48] This prompt reporting enables swift action to mitigate potential data breaches and protects customers' sensitive information. The Guidelines set transaction limits (N15,000) and daily cumulative limits (N50,000) for contactless payments, requiring customer verification for transactions above these limits.[49] This measure safeguards customers' accounts and prevents unauthorized transactions. The Guidelines provide customers with an opt-out option for contactless payment products, ensuring customers' autonomy over their financial transactions. Additionally, issuers must obtain customer consent before activating contactless payments.[50] The Guidelines require switching companies to enter service level agreements with stakeholders, specifying responsibilities,

---

46 Olaniwun Ajayi LP, 'CBN Issues Draft Guidelines on Contactless Payment in Nigeria' (8 November 2022) available at <https://www.olaniwunajayi.net/blog/wp-content/uploads/2023/07/Newsletter-OVERVIEW-OF-THE-CBNS-GUIDELINES-FOR-CONTACTLESS-PAYMENTS-IN-NIGERIA-2023-002-1.pdf> accessed 10 September 2024.

47 Regulation 5.5 of the Guidelines.

48 Regulation 5.6 of the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018 and Regulation 7.6 of the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions, 2022.

49 Regulation 9.5 of the Guidelines.

50 Switching companies refers to CBN-licensed financial institutions that operate an electronic system that captures electronic financial transactions from touch-points, applies rules, determines destinations, delivers the transactions and gives appropriate feedback. See Regulation 5.0(14) of the CBN's Guidelines on Transactions Switching in Nigeria 206.

operational rules, and liabilities.[51] This clarity ensures that parties understand their roles in protecting customer data.

CONCLUSION

The rapid development of technology and the growing usage of personal data have sparked global worries about privacy and data protection. Nigeria, the most populated nation in Africa, has implemented several laws and regulations to address these issues.

For further information on this article and area of law,
Please contact **Ibukun Spaine** at:
S. P. A. Ajibade & Co., Lagos by
Telephone (+234 1 472 9890), Fax (+234 1 4605092)
Email: www.spaajibade.com

[51] Regulation 6.5.3. of the Guidelines.