CORPORATE RESPONSIBILITY AND DATA PRIVACY UNDER THE NIGERIA DATA PROTECTION ACT: LEGAL OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS

Chinazor Queen Umeobika,[*]
Linda Amarachi Oti-Onyema[**]
and Chipuruime Obiagwu[***]

Abstract

The demand for and generation of personal information of individuals by corporate entities are accelerating with the advancement and engagement of technology, in the regulation of human activities. According to Statista, the amount of information created, copied, captured and consumed worldwide will go from 120 zettabytes in 2023 to 181 zettabytes in 2025. (One zettabyte is one trillion gigabytes.)[1]As data continues to be released and sometimes shared amongst interrelated organisations, their exposure and manipulation by unwanted, unscrupulous elements increase. The criminal activities of hackers to access and exploit data residing with these organizations are on a rampage, that it is gradually becoming difficult to manage data against illegal interference, thereby raising data security concerns. This Article studied the obligations of corporations engaged in controlling and processing personal data by a doctrinal research approach. It was found that data privacy has not received the desired protection in Nigeria despite the enactment of the Nigerian Data Protection Act, largely due to a lack of awareness of the relevant laws. It was therefore recommended that periodic sensitization programs and training be organized for the management and staff of these data corporations, as well as the public on their rights, obligations and sanctions for non-compliance with Data Privacy Laws.

Key Words: Corporate Responsibility, Data Privacy, Best Practices, Data Subjects, Data Controllers

1. Introduction

For efficient service and product delivery, data subjects[2] are often required to submit certain data to their service providers. This could be personal or sensitive data, like the Card Verification Value (CVV) of an Automated Transfer Machine Card. It is interesting to note that some corporations, which include data processors and controllers, now unethically handle this data at the expense of the data subject or owner. Sometimes, exposing these data owners or subjects to unbearable risks, particularly in the face of huge insecurity challenges in the country. It is no news that many cases of hostage taking, fraud, and cybercrimes have been masterminded by insiders in corporations that have access and control the personal data of members of the public. Unfortunately, in certain cases, citizens are under a legal obligation to submit and sometimes, surrender these data to such corporations with no corresponding

[*] **Associate Professor Chinazor Queen Umeobika**, **Ph.D** (Reader and Head, Private and Property Law Department, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State), cq.umeobika@unizik.ng
[**] **Linda Amarachi Oti-Onyema, Ph.D**, Lecturer, Faculty of Law, Nnamdi Azikiwe University, Awka la.oti-onyema@unizik.ng
[***] **Chipuruime Obiagwu**, **Esq**., Lecturer, Imo State University, Owerri, obiagwuchipuruime@gmail.com
[1] Amount of Data Created Daily(2025), <https://explodingtopics.com/blog/data-generated-per-day> accessed on 11/5/2025
[2] *Section 65* NDPA

duty on the corporations to safeguard those data. Efforts have been made by the Nigerian government in the past to create a legal framework for data privacy. The Constitution of the Federal Republic of Nigeria[3], Cybercrimes (Prohibition, Prevention, etc.) Act[4], Freedom of Information Act[5], Nigeria Data Protection Regulation 2019 etc. are some of the laws and regulations put in place by the government to protect data in the public domain. While these efforts are commendable as the threshold for the new legislation on data, the Nigeria Data Protection Act[6], they were not adequate to secure the privacy of data subjects and owners against data manipulators and hackers and to regulate the activities of data controllers and processors regarding the date in their possession; hence, the enactment of the NDPA. This Article is an attempt to examine the legal obligations of data processors and data controllers with respect to data privacy *vis-à-vis* internationally established practice.

2. Clarification of Concepts

2.1 Corporate Responsibility

Corporate Responsibility is the incorporation of ethical elements, such as the public interest and environmental concern, into the planning of business strategy[7]. It refers to the responsible acts expected of and from corporate bodies, which are in this work, denoted as data processors and data controllers. Responsible here relates to acts that denote or show a sense of integrity and awareness of one's environment. Things done without immediate consideration of one's environment and space are deemed irresponsible acts. When corporate bodies undertake acts that cater to or care for their environment, those acts are called corporate responsibility. One great aspect of corporate responsibility is compliance with human rights laws. In *Kiobel v Royal Dutch Petroleum Co*.[8] In this case, the United States Supreme Court recognized the Alien Tort Statute as a means to hold corporations accountable for human rights abuses committed abroad. The ruling emphasized that corporations can be held liable for their complicity in human rights violations. Similarly, in *Vedanta Resources plc v. Lungowe*[9] the United Kingdom Supreme Court ruled that a parent company could be liable for the actions of its subsidiary in another country, if it failed to prevent human rights and environmental harms.

2.2 Data Privacy

At the substratum of reliable information is quality data. Data is information such as facts and numbers used to analyze something or make decisions.[10] Data privacy, sometimes referred to as information privacy, is an area of data protection that concerns the proper handling of sensitive data including, notably, *personal data* but also other confidential data, such as certain financial data and intellectual property data, to meet regulatory requirements as well as protecting the confidentiality and immutability of the data.[11]The essence of data privacy is, in the main, to protect the data and details of users who have granted data processors and data controllers access to their data. This is to ensure the data so supplied do not fall into the hands of miscreants or be exposed to entities who may use them for ulterior purposes. The key

3 1999 (as Amended)
4 2015
5 2011
6 (NDPA) 2023
7 Corporate Responsibility, < https://www.collinsdictionary.com/dictionary/english/corporate-responsibility>accessed on 21 October,2024.
8 569 U.S. 108 (2013)
9 [2019] UKSC 20
10 < https://www.vocabulary.com/dictionary/data> , accessed on 21 October,2024.
11 <https://www.snia.org/education/what-is-data-privacy> , accessed on 19 September,2024.

components of data privacy are: data confidentiality, data security and transparency in data usage.[12]

Data confidentiality: This refers to the concept that data, once shared with data processors and data controllers, should not be made subject to public scrutiny without the consent of the user. This consent must be obtained expressly, and disclosure of this data must be in consonance with the tenets of good conscience and equity. Hence, terms and conditions drafted by the corporation must adhere and align with the rights of every citizen to their privacy.[13]

Data Security: This focuses on protection of the data supplied to data processors and data controllers from hacking, and illegal access or usage. For instance, users of Google must have an assurance that their personal and confidential data, which they have shared with the Corporation, are safe from being maliciously hacked and also secure from cyber criminals. If this sense of security is not in place, Google will lose its users and clients and in the long run reputation and income. Data security is an important aspect of data privacy.

Transparency in data usage: This concept charges corporations to foster clarity in their terms and conditions of usage to be accepted by end users of their products. Clarity here refers to the ease of understanding the language and its usage. In an instance where a corporation inserts legal jargons in its terms of service, it is not deemed an ethical practice as other common synonyms are easily understood by non-lawyers that should be used. The language used should also be a lingua franca for the corporation's target audience, as this is to ensure understanding and ease of communication. It is unimaginable that a term and condition for service written in English for a purely traditional French audience or vice versa, such an agreement would not have met the transparency for data usage standard.

2.3 Data Controller and Data Processor

A "data controller" means an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data.[14] A "data processor" means an individual, private entity, public authority, or any other body who processes personal data on behalf of or at the direction of a data[15]From the definition, data controllers and processors can be individuals or corporate bodies who in the main process data. Data processors and data controllers are major actors in the field of data privacy,

3. Historical Background of Data Privacy in Nigeria

Data privacy is an aspect of data protection and its origin cannot be severed from the origin of data protection in Nigeria. The concept of data protection in Nigeria owes its origins to the incursion of technology in the country's economic activities when the erstwhile communal standard of living characteristic of the Nigerian societies, like their African counterpart, had given way to the realization of the importance to protect personal information from untoward use, at a time when the importance of (personal) data to most businesses had become more intrinsically pronounced.[16]

---

12 <https://www.secoda.co/glossary/data-privacy > <accessed on 19 September, 2024.

13 *Section 37*, Constitution of the Federal Republic of Nigeria, 1999 (as amended)

14 *Section 65* of the NDPA

15 *Ibid*

16 Olumide, B., 'Nigeria's data protection legal and institutional model: an overview', *International Data Privacy Law*, [2022], Volume 12, Issue 1, 44–52

The first legislative attempt at regulating data privacy is the Constitution, which guarantees the right to privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications.[17] The infringement of this right can be challenged in court and redressed where meritorious.[18] However, several other attempts have been made to address fragments of data privacy violations such as the Cybercrimes (Prohibition, Prevention, etc.) Act, Freedom of Information Act and Nigeria Data Protection Regulation 2019.

Prior to these legislations and regulations, frantic efforts had been made to provide a specific law to regulate data privacy in Nigeria. In 2005, the Computer Security and Critical Information Infrastructure Protection Bill was sponsored, but it was unsuccessful. However, the bill resurfaced in 2011 but was withdrawn before completing its legislative cycle.[19] The next verifiable legislative attempt was the Data Protection Bill 2010 targeted at 'reducing' unauthorized processing and use of personal data and information without the prior consent of the data subjects.[20]The bill was reputed to be the first federal legislative proposal wholly focused on data protection but after scaling the first reading, nothing was recorded or heard of the bill again. Other failed attempts include the Nigerian Data Protection Bill, the 2013 (draft) Guidelines on Data Protection, Data Protection Bill 2020.[21] However, due to the indispensable need for a specific law on Data privacy and protection, the National Assembly in 2023, passed into law the current Nigeria Data Protection Act.

4. Legal Obligations of Corporations under the NDPA 2023

In the course of carrying on its objects, data processors and data controllers come in contact and utiltise data owned by individuals, other corporate bodies, government of States and the like, who are referred to as data subject. At the base of information and its utilization is data. Data can be drawn from surveys, questionnaires, programs, subscriptions, website visits etc. and as with the emerging times and rapid technological advancement we now operate in, data subjects share and grant access to their personal data without mostly, carefully perusing the fine prints of the terms and conditions they must accept. Consequently, data processors and data controllers build reliable database off the data of willing and most times, unwilling data subjects. Except such data processors and data controllers have a high reliance on its ethical values, there is a propensity for disuse and abuse of such data within its control. Expectedly, most developed and developing States have evolved strong laws and legal regimes guiding the usage and dissemination of data. In Nigeria, the National Assembly has enacted the Nigeria Data Protection Act (NDPA) in 2023 aimed at providing for the legal base from which individuals and corporations must act when handling. In the main, the Act seeks to protect the fundamental right to privacy of data subjects.[22] This right is to know and approve of everything that happens to his data. The Act created circumstances where this Act is inapplicable, such as when a competent authority carries out data processing for the prevention, investigation, detection, prosecution, or adjudication of a criminal offence or the execution of a criminal penalty, or as is necessary for national security.[23] However, the exemptions are made subject to the fundamental rights of the Data Subject.[24] In *Jose Alvear Restrepo Lawyers' Collective v. Colombia*[25], the case challenged the systematic surveillance

17 *Section 37* of the Constitution
18 *Section 46* of the Constitution.
19 Olumide B, *op.cit.*
20 *Ibid*
21 *Ibid*
22 *Proviso* Section 3(1), NDPA.
23 *Section 3(2)(a) &(c)of the Act*
24 *Section 3(2)*
25 Petition 12.380, Inter-Am. C.H.R., Report no. 55/06

carried out against the José Alvear Restrepo Lawyers' Collective (known as its acronym in Spanish, CAJAR), a non-governmental organisation led by lawyers who specialise in claimant-side human rights litigation in Colombia. The Court determined that since the 1990s several state bodies carried out arbitrary intelligence activities to the detriment of the members of CAJAR and their next of kin. In this context, the authorities gathered information, including personal data, based on which they prepared personal files including notes and records on the victims. To date, the victims have not been granted access to those intelligence records, thus prohibiting them from requesting any update, correction or elimination of their data, as applicable. The intelligence activities continued while Law No. 1621 of 2013 was in effect, which aimed to regulate the functions of the intelligence and counter-intelligence bodies. Moreover, the members of CAJAR were subject to stigmatization due to statements made by government officials and publications by government offices that disqualified them and linked them to guerrilla groups. The surveillance measures deployed against CAJAR forced members to limit their activities, change their domicile, and in extreme cases left them with no option but exile due to the acts of violence, threats, and harassment they suffered as a result of state intelligence operations. The Inter-American Court of Human Rights declared that the Republic of Colombia internationally responsible for human rights violations against several members of the CAJAR and their relatives. The Court noted that the autonomous right to informational self-determination derives from the contents of the American Convention on Human Rights, including the right to access and control personal data in public files.

4.1.1 Who must Protect Data Privacy?

The Act has specified who is responsible for guaranteeing data privacy. The obligations under the Act shall apply only to data controller or data processor who

a. is domiciled in, resident in, or is operating in Nigeria;
b. processes personal data within Nigeria; or
c. is not domiciled in, resident in, or operating in Nigeria, but is processing personal data of a data subject in Nigeria.[26]

As earlier expressed above, a data controller or processor may be a natural or an artificial entity. Therefore, corporate bodies involved with data processing and controlling, domiciled and operating[27] within Nigeria, and those though, not domiciled or operating in Nigeria but process data of a subject so domiciled, must be guided by the provisions of this Act. Invariably, no claim can lie against data controlled or processed outside Nigeria except in the circumstances mentioned in *Section 2(2)*© of the Act. Note that the Act applies to data controllers and processors of both automated and unautomated data.

For a successful claim against violation of one's right to privacy of his data, the court must determine first, if the Defendant is a data controller or processor as defined by the Act. In *Olamide Babalola LP v True Software Scandinavian AB*[28] the applicants sought the court's determination on whether Truecaller's collection, storage, and processing of the personal data of non-users of the app without first obtaining their consent is likely to interfere with their rights to privacy and whether it violated the provisions of Regulation 2.1 and 2.3 of the Nigeria Data Protection Regulation, 2019. The Federal High Court stated that the phone owners (users) are the data controllers. Truecaller did not unilaterally collect or harvest the phone numbers of the applicants; rather, it is the data controller who gave consent and access to these phone numbers. Without the action of the data controllers, Truecaller would have no access

[26] *Section 2(2), NDPA*.
[27] Processing data
[28] *(2024) 6 CLRN*

to the applicants' personal details. The court ruled that Truecaller does not operate as a data controller or harvester of phone numbers. The court stated that fault lies with the data controller and not the respondent, who, without the action of the controller, would have no access to these details, and that the app does not operate as a collector of phone numbers. "The application is used to trace the identity or origin of unknown callers. The identity is revealed if contained in the database of the application. This, to my mind, does not amount to infringement of the right to privacy."

4.2 Qualification for Data Processing and Controlling Under the Act

To be competent to receive, process and control personal data of citizens of the country, a person must be duly registered with the Nigerian Data Protection Commission. According to *section 44(1)* of the NDPA, data controllers or processors of major importance, subject to higher obligations and penalties, are required to register with the NDPC six (6) months after the commencement of the Act or upon attaining this status.[29] This is a legal obligation as stipulated by the Act. As one of its functions, *Section 5(d) of the Act* authorizes the Commission to register data controllers and data processors of major importance. The essence, is to make room for the organisation and generation of a reliable database of data processors in Nigeria. The rationale behind the limitation of the registration requirement to only data controllers and processors of importance and the classification of data controllers and processors into important and unimportant is far beyond reach.

More worrisome is the provision of *subsection (6)*, which empowers the Commission to exempt a class of data controllers or data processors of major importance from the registration requirements, where it considers such requirement to be unnecessary or disproportionate. Although *section 65* of the Act attempted a definition of "data controllers and processors of importance", it is still difficult to decipher the meaning of the term. *Section 65* of the Act defines "data controller or data processor of major importance" to mean "a data controller or data processor that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate."

Generally and by *section 3(3)* of the NDPA, the Commission may by regulation prescribe types of personal data and processing that may be exempted from the application of this Act. The exemption granted to any data controller or processor does not exonerate them from operating lawfully and legally and does not remove them from the regulatory powers and watchful eyes of the Commission. To this point, *Section 3(4)* empowers the Commission issue a guidance notice containing legal safeguards and best practices to a data controller or processor, in respect of any aspect of data processing exempted where in the opinion of the Commission, such processing violates or is likely to violate *sections 24* and *25* of the Act.

The discretion given to the Commission to exempt a class of data controllers or processors is very dangerous, considering the high tendency and rate of corruption in the country. The Act ought to outline modalities for the exercise of the discretion. Again, the Act gave discretion to the Commission to prescribe a data controller or processor who can be classified as of major importance where the data to be processed is more than such number of data subjects within Nigeria.

[29] Section 44(1), NDPA.

Riding on these provisions, the NDPA released the Guidance Notice on the Registration of Data Controllers and Processors of Major Importance in 2024. The Guidance Notice specified persons who can be regarded as Data Controller/Processor of Major Importance. A Data Controller or Data Processor that has particular value or significance to the economy, society, or security of Nigeria and keeps or has access to a filing system (whether analogue or digital) for the processing of Personal Data and carries out any of the following is designated as a DC/PMI:

a. Processes the Personal Data of more than 200 (Two Hundred) Data Subjects in six months; or
b. Carries out commercial Information Communication Technology (ICT) services on any digital device which has storage capacity and belongs to another individual;
c. Processes Personal Data as an organisation or a service provider in anyone of the following sectors:
    i. Financial
    ii. Communication
    iii. Health
    iv. Education
    v. Insurance
    vi. Export and Import
    vii. Aviation
    viii. Tourism
    ix. Oil and Gas
    x. Electric Power

A Data Controller or Data Processor (DC or DP) who is under a fiduciary relationship with a Data Subject by reason of which it is expected to keep confidential information on behalf of the Data Subject shall be regarded as a DC/PMI taking into consideration the significant harm that may be done to a Data Subject if such Data Controller or Data Processor is not under the obligations imposed on a DC/PMI.

The extent of the exercise of this discretion to exempt from registration and application of the Act of Data controllers and processors has been subject to controversies, which have been recently tested in court. It has been contended that the discretion given to the Commission does not extend beyond prescribing a data controller or processor who processes or intends to process data that is more than such number of data subjects within Nigeria. In *Frank Ijege v. Nigeria Data Protection Commission,*[30]the case was brought before the FHC in Kaduna State. Mr. Frank Ijege, the applicant, sought several reliefs, including a declaration that the Guidance Notice violated his right to privacy, a clarification of the Notice's confusing provisions, and a statement that not all individuals or entities qualify as (data controller or data processor of major importance (DCPMI).

The applicant challenges the legality of paragraph 1 (2) of the Guidance Notice, arguing, among other things, that its enactment exceeds the powers granted to the NDPC under the NDPA. Specifically, the applicant contends that, in light of *sections 3 and 65* of the NDPA, the challenged provision falls outside the scope of authority contemplated by these provisions and should therefore be invalidated. In response to the applicant's argument, counsel for the NDPC contended that paragraph 1(2) of the Guidance Notice does not contravene *section 65* or any other provision of the NDPA. Counsel further argued that the applicant had failed to

[30] (FHC/KD/CS/34/2024

provide any cogent explanation to show how 'almost every citizen is involved with one another in a fiduciary relationship with one another to the extent that every human and artificial person would be a data controller and processor of major importance'. He emphasized that accountability, as a threshold principle, is explicitly provided for in the NDPA, particularly in *section 24*, and is not a creation of the Guidance Notice. On these grounds, among others, counsel urged the Court to dismiss the suit as lacking in merit.

In its analysis, the Court, however, sided with the applicant, holding that the fiduciary relationship element ascribed to a data controller or data processor of major importance under paragraph 1(2) of the Guidance Notice does not align with the criteria enumerated in *section 65* of the NDPA. The Court noted that *section 65* provides a definitive framework for identifying data controllers or processors of major importance and does not include fiduciary relationships as one of the defining factors. This, according to the Court, is 'because fiduciary relation could merely be personal'.

This decision of the Federal High Court has been criticized by some scholars, but suffice it to note that the power of exemption granted to the Commission is both general and specific. The first is found in *section 3* relating to types of personal data, while the specific one relates to exemption of data controllers and processors. While the former deals with the data itself and the application of the Act to it, the latter deals with holders of such data and their registration. A good understanding of this would help in arriving at a sagacious conclusion of whether or not the Commission exceeded its powers in the Guidance Notice.

From the above definition, it presupposes that any person or institution whose data processing or control does not affect the national interest is not of major importance and therefore, not under any duty to register with NDPC. A little stretch of this would mean that personal data used for private purposes does not require the registration of its processors or controllers. It is submitted that all data in possession or custody of any person other than its owner (be it a private person or public institution) should be regulated and bound by the provisions of the Act without exemption. Again, the dichotomy between data of importance and unimportance should be erased.

4.3 Obligations of the Data Controllers and Processors

One of the objectives of the NDPA is to ensure that data controllers and data processors fulfil their obligations to data subjects[31]. This unambiguous provision of the Act settles every controversy about whether data controlling and processing corporations have an obligation to protect data privacy.

The NDPA's mandate is not just to guarantee data privacy rights to data subjects but to establish a framework for the realization of these rights. It will not be out of place to submit that the objectives of the Act, as expressed *in section 1(f)*, are for the enforcement/implementation of data rights. Where data controllers and processors fulfil their duties to data subjects, data rights are implemented.

It is therefore important to study the Act to know the extent to which it has enabled the fulfilment of the obligations of data controllers and processors.

a. Duty of Compliance

By *section 29(a)* of the Act, where a data controller engages the services of a data processor, or a data processor engages the services of another data processor, the data

[31] *Section 1(f)*

controller or data processor engaging another shall ensure that the engaged data processor- (a) complies with the principles and obligations set out in this Act as applicable to the data controller. A data controller or processor must not be in default or defiance of the rules and responsibilities under the Act. In fulfilment of their obligations under the Act, the data processor or controller shall engage and provide appropriate information, technical and organizational measures, particularly to ensure the security, integrity, and confidentiality of personal data.[32]

b. Duty of legality and transparency

Section 24(1)(a) of the Act mandates a data controller or processor to ensure that personal data is processed in a fair, lawful and transparent manner. The Act does not define fair or transparent data processing, unlike the requirement for data processing to be lawful, which was defined in *section 25 of the Act*. However, a look at the European Union's Data Protection Regulation can guide us in understanding the concepts of fair and transparent processing. The principle of transparency is an expression of good faith when processing personal data.[33]The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. [34]The controller should provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data is processed. [3] Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. [4]

The lawfulness of data processing is determined by the factors outlined in *section 25* of the Act where:

a. the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed. Recently, the Federal High Court in Abuja ruled against the use of a person's personal data without his consent. In *Araka v Ecart Internet Services Nigeria Limited & Anor*[35]the case began in March 2023 when Akosa Araka placed an order through Jumia Food. His personal data was collected solely to facilitate the transaction. However, Domino's Pizza later repurposed his data for unsolicited marketing messages without his consent. Between December 2023 and May 2024, Akosa received a total of 16 unwanted marketing messages despite repeatedly requesting the cessation of the unsolicited messages. His pleas fell on deaf ears, thereby prompting him to pursue legal action. During the hearing, the court learned that Jumia Food had shared Akosa's details with Domino's Pizza as part of an On-Demand Service Agreement (ODSA) between both companies. However, Domino's did not have permission to use that data for marketing purposes. In its ruling, the Court established that Domino's Pizza had violated *Section 37* of Nigeria's Constitution and *Sections 25 and 26* of the Nigeria Data Protection Act (NDPA) 2023 by processing Akosa's data unlawfully. The court emphasised that Domino's Pizza acted as a data processor under the NDPA and had no legal right to repurpose Akosa's data without consent. Jumia Food fulfilled its duty of care by warning Domino's to stop processing the customer's data. Domino's was solely liable for the continued misuse

32 See subsections b, c and d

33 Data subjects' rights, GDPR principles, <https://www.activemind.legal/guides/transparency-processing/> accessed on 7/5/2025

34 General Data Protection Regulation (GDPR) of the European Union 2018

35 Unreported Suit N0 FHC/ABJ/195/2025

of Akosa's information and for ignoring his formal request to be removed from their database.

In the Kenyan case *of Mwonga & 4 others v Ogega & another*[36] the Petitioners, whose graduation photographs were used without consent by a private college to advertise its academic programs sued for enforcement of their rights to privacy of their data in the custody of the College. The images were shared widely across social media platforms, brochures, banners, and billboards – actions that violated constitutional rights and exploited their data for commercial gain. *The Court ruled in* favour of the petitioners, holding that the unauthorized use of the Petitioners' images violated their constitutional rights to dignity and privacy under Articles 28 and 31 of the Constitution and their intellectual property rights. Each Petitioner was awarded compensation for the unlawful use of their images and the Court issued a permanent injunction, directing the Respondents to cease using the Petitioners' images for any commercial purposes and to remove all promotional content featuring the images immediately. The judgment reinforced the importance of adhering to the Kenyan Data Protection Act of 2019, which mandates explicit consent from data subjects and restricts the use of personal data beyond its intended purpose.[37]

b. the processing is necessary-

(i) for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract,
(ii) for compliance with a legal obligation to which the data controller or data processor is subject,
(iii) to protect the vital interest of the data subject or another person,
(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or
(v) for the purposes of the legitimate interests pursued by the data controller or data processor, or by a third party to whom the data is disclosed.

To avoid abuse of *subsection (1)(b)(v)*, the Act circumscribed its application by stating limits beyond which such legitimate interest cannot go. Thus, interests in personal data processing shall not be legitimate where they override the fundamental rights, freedoms and the interests of the data subject; they are incompatible with other lawful basis of processing under subsections (1)(b) (i)-(iv); or the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

c. Duty to disclose and maintain the purpose for the Data collection or processing

By the provisions of *section 24(1)(b)*, the data controller or processor must ensure that personal data **is** collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes. The Data controller must state in clear terms the purpose to which the personal data is to be used. Additionally, the data controller or processor must limit its operation to the personal data collected or further processed. A data controller or processor is, therefore, under a duty to refrain from using the data against or *beyond* the purpose for which it was provided. Additionally, data should be retained for not longer than is necessary to

[36] [2024] KEHC 16469 (KLR)

[37] Landmark Judgment on Data Privacy and Dignity in Kenya, <https://njagaadvocates.com/landmark-judgment-on-data-privacy-and-dignity-in-kenya/ >accessed on 7/5/2025

achieve the lawful basis for which the personal data was collected or further processed.[38]

d. Duty to ensure accurate and complete data

Section 24(1)(e) imposes a duty on the data controller and processor to ensure the personal data is accurate, complete, not misleading, and, where necessary, kept up to date, having regard to the purposes for which the personal data is collected or is further processed.

e. Duty to Secure Personal Data

Data collectors and processors must ensure data is processed to ensure its appropriate security, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.[39] *Section 39* equally mandates that "a data controller and data processor shall implement appropriate technical and Security, and organisational measures to ensure the security, integrity and confidentiality of and confident personal data in its possession or under its control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access.

Data security is a fundamental prerequisite for ethical and fair data processing. To foster the propagation of innovations, questions related to security concerns must first be successfully addressed. Corporations should integrate security best practices into their modus operandi at the organisational level (in terms of building a culture of security awareness, secure behaviours and procedures inside the Organisation) and the technical level (in terms of information technology (IT) processes, the design of products and services, which should take security into account).

The principle of Data Security calls for the implementation of a risk-based approach to data processing that aids in the management of data security to optimise economic and social benefits expected from digital openness. This means that for society to take full advantage of and benefit from technological advancements, the risks posed by such technologies in terms of security must first be successfully mitigated. The identification, quantification, and management of risk assists in adequately balancing the 'opportunities for gains and minimizing vulnerabilities and losses.[40]

The zero-trust model to security should be adopted by the Organisation, meaning that the Organisation 'should not automatically trust anything (actors, systems, or services operating) inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access.'[41] Resilience should

38 *Section 24(1)(d)*

39 *Section 24(f)*

40 Enisa, "Guidelines for SMEs on the security of personal data" <processinghttps://www.enisa .europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> accessed on 10/5/2025

41 Josh Fruhlinger, "What is zero trust? The security model for a distributed and risky era", <https://www. csoonline.com/article/564201/what-is-zero-trust-a-model-for-more-effective-security.html >accessed on 10/5/2025

be ensured, as should the ability of the Organisation to react quickly to breaches and of course, any potential threats and risks that may arise in the course of time.[42]

f. Duty of Confidentiality and Integrity

A data controller and data processor shall use appropriate technical and organisational measures to ensure the confidentiality, integrity, and availability of personal data. [43]

g. Duty of Care:

Data controllers owe the data subjects a duty of care on how they handle the data so collected. A data controller or data processor owes a duty of care, in respect of data processing, and shall demonstrate accountability, in respect of the principles contained in this Act.[44]

Right to privacy, including data privacy, is the fundamental right of a data subject. In handling of such data, data processors and controllers are to act accordingly, with the relevant section of the Constitution and Act.

h. Duty to Sensitive Personal Data:

It is the legal obligation of a data controller or processor to ensure that consent of a data subject is obtained and not withdrawn prior to processing of such data.[45] It is also pertinent to add that it is the obligation and corporate responsibility of a data processor or controller to ensure that the sensitive data sought to be obtained conforms with the provisions of *Section 30 (1)* of the NDPA including the processing being necessary for the purposes of performing the obligations of the data controller.[46]

i. Protection of rights of the Data subject.

The data controllers and processors, as its legal obligation and aspect of its corporate responsibility, must ensure that the rights of data subjects as enshrined in Part VI of the NDPA are protected. This is in fact the fulcrum on which data privacy and regulations rests flowing from Section 37 of the Constitution of the Federal Republic of Nigeria (1999 as amended). A data subject has rights that must be protected and this includes right to privacy of their data, despite consenting to its processing by the data controller. Some of these rights include,

i. a data subject has the right to obtain from a data controller, without constraint or unreasonable delay,[47]
ii. a data subject shall have the right to withdraw, at any time, consent to the processing of personal data under this Act,[48]
iii. a data controller shall discontinue the processing of personal data, unless the data controller demonstrates a public interest or other legitimate grounds, which overrides the fundamental rights and freedoms, and the interests of the data subject,[49]

---

42 UM-DPCSR Framework Principle 1: embed data protection, fairness, and security in the design of processes<file:///C:/Users/hp/Downloads/9781035314164-chapter4.pdf>accessed on 10/5/2025
43 *Section 24(2)*
44 *Section 24(3)*
45 *Section 30*, NDPA
46 *Section 30 (1)* b, NDPA.
47 *Section 34(1)*, NDPA
48 *Section 35(1)*, NDPA
49 *Section 36(2)*, NDPA

iv. where personal data is processed for direct marketing purposes, the data subject shall have the right to object, at any time, to the processing of personal data concerning the data subject, which includes profiling to the extent that it is related to such direct marketing,[50]

v. a data subject is entitled to right of data portability under this Act[51]. Data portability in the, main refers to ease of transmission of data belonging to the data subject.

5. Legal Consequences for Non-Compliance with the Act

Both criminal and civil action can be initiated, even simultaneously, against a defaulting data controller or processor. Notwithstanding any criminal sanctions under this Act, NDPC, if satisfied after investigation, that a data controller or data processor has violated any provision of this Act or subsidiary legislation made under this Act, it may make any appropriate enforcement order or impose a sanction on the data controller or data processor. An enforcement order made or sanction imposed shall include —

(a) requiring the data controller or data processor to remedy the violation;
(b) ordering the data controller or data processor to pay compensation to a data subject, who has suffered injury, loss, or harm as a result of a violation;
(c) ordering the data controller or data processor to account for the profits realised from the violation; or
(d) ordering the data controller or data processor to pay a penalty or remedial fee.

By *section 49. (1)* a data controller or data processor who fails to comply with orders made by the Commission commits an offence and is liable on conviction to penalties. Section 51 grants a data subject the right to seek civil remedies. Thus, a data subject who suffers injury, loss, or harm as a result of a violation of this Act by a civil remedies data controller or data processor may recover damages from such data controller or data processor in civil proceedings. Notwithstanding anything to the contrary, the Court may make an order of forfeiture against a convicted data controller, data processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act.[52]

6. Conclusion/Recommendations

The need for corporate bodies, which in this essay are termed data controllers or data processors, to act in compliance with the provisions of the NDPA cannot be overstated. Such compliance is a strong form of corporate social responsibility expected by data controllers or processors, as data privacy and protection are the fundamental rights of persons within the country.

The specific legal obligations and acts accounting for corporate responsibility to data privacy for data controllers and data processors have now been narrowed down with the enactment of the Nigeria Data Protection Act (NDPA) in 2023.

It now behoves these data controllers and processors to act in alignment with the provisions of the Act and other attendant regulations of the Nigeria Data Protection Commission.[53]Although some persons are beginning to resist through legal actions any

[50] *Section 36(4),* NDPA
[51] *Section 38(2),* NDPA
[52] *Section 52*
[53] *Sections 4* and 5, NDPA.

violation to their rights, greater number of the populace are in the dark concerning data privacy and protection.

It is therefore, recommended that periodic sensitization programs and training should be organized for the management and staff of these data corporations, as well as the public on their rights, obligations and sanctions for non-compliance with Data Privacy Laws.

It is further recommended that all data in possession or custody of any person other than its owner (be it a private person or public institution) should be regulated and bound by the provisions of the Act without exemption. Again, the dichotomy between data of importance and unimportance should be erased