THE FOUNDATION OF DATA PROTECTION: EXPLORING NIGERIA'S KEY PRINCIPLES

Emmanuel Tochukwu OKPARA, Onyegbule Kelechi G[1]

Abstract

In today's digital landscape, safeguarding personal data has become a pressing concern for individuals, businesses, and the government. This paper explores the fundamental principles of data protection as established by Nigeria's Data Protection Act (NDPA) of 2023. It delves into the core principles of data protection as contained in the NDPA, including lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality and accountability. With reference to other jurisdictions like Europe, a comprehensive analysis of these principles was made, highlighting their significance in the Nigerian context and their role in ensuring that data controllers and processors operate in compliance with required standards. The NDPA marks a crucial shift in Nigeria's approach to data governance, enhancing the rights of data subjects while fostering accountability in the handling of personal data. This analysis provides insight into how these principles aim to balance privacy protection with the operational needs of organizations, thereby strengthening trust and security in Nigeria's growing digital economy.

Keywords: Data Protection, Foundation, GDPR, NDPA, Nigeria, Principles.

INTRODUCTION

BACKGROUND

Where a comprehensive data protection law exists, organizations, public or private, that process personal information have an obligation to handle these data according to data protection law; in Nigeria an example of such law is the Nigeria Data Protection Act, 2023.[2] Derived from regional and international frameworks, a number of principles should be abided by when processing personal data.[3]

There are universally accepted principles that govern the protection of data and personal information. The need for observance of these principles is highlighted by the upsurge of modern technologies which have invariably disrupted the mode of communication, implicated the nature and relevance of information, as well as reinforced the need to safeguard the right to privacy in an era of invasive innovations.[4] In tune with international standard, NDPA recognizes the following basic principles which must be observed in the processing of personal data;

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Data accuracy
5. Storage limitation
6. Data security/integrity and confidentiality
7. Accountability

[1] Emmanuel Tochukwu Okpara; Data Protection and Privacy Consultant, Lecturer at Department of Criminology and Security Studies, University of Agriculture and Environmental Science, Umuagwo, Imo State, Nigiera. emmanuel.okpara@uaes.edu.ng, +234 806 0707 269

Onyegbule Kelechi Goodluck, LL.B, BL, LL.M(Oil and Gas), Ph.D(Medical Law), Head of Department of Public and Private Law, Alex Ekwueme Federal University, Ebonyi State, Founder; Leeds Legal, Fellow, Institute of Medical and Health Law, Nigeria and Medical Law Consultant. onyegbule.kelechi@funai.edu.ng, +2347034275817;

[2] Herein after referred to as NDPA.

[3] Privacy International, A Guide for Policy Engagement on Data Protection, Part 3 Data Protection Principles<https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf> Accessed 25 August, 2023.

[4] Alexender Asuquo, The Principles of Nigeria Data Protection Law <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3408775> Accessed 28th August, 2023.

RESEARCH METHODOLOGY

The method of research adopted in this research work is, the doctrinal method which involves gathering of information from materials useful to this work. Materials relevant to this work includes but not limited to; The Constitution of the Federal Republic of Nigeria 1999 (as Amended 2023), authoritative writings like text books, dictionaries, journals, articles, and handouts etc., of scholars who are vast in the knowledge of the constitution, and also law reports was sourced to enrich this work.

PRINCIPLES OF DATA PROTECTION

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY: The principle of lawfulness, fairness and transparency holds a central position in data protection. This is because the lawfulness, ethics and transparency of processing indeed find root in this principle. This principle is key to addressing practices such as the selling and/or transfer of personal data that is fraudulently obtained. 'Fairness and transparency' are essential for ensuring that people's data is not used in ways they would not expect.[5] The NDPA[6] provides that a data controller or data processor shall ensure that personal data is; processed in a fair, lawful and transparent manner and for specified, explicit, and legitimate purposes, and not be further processed in a way incompatible with these purposes. By *Section 24(1)(a) & (b)* of the Nigerian Data Protection Act, personal data must be collected and processed in accordance with specific, legitimate and lawful purpose consented to by the data subject. These requirements of fairness, specificity, legitimacy and lawfulness are in addition to other procedures laid down in the Act or any other instrument.

The purport of this principle generally is that controllers must in the first place have legal grounds for processing personal data and secondly, never use such data in a manner which may have unjustified consequences for the persons concerned and thirdly, proactively disclose information on the legal grounds for the data processing.[7]

Lawfulness of processing: This requires personal data to be processed lawfully by a data controller identifying at least one legal ground for processing personal data. For processing to qualify to have been done on lawful or legal basis, personal data must be processed only on the basis of one of the following grounds, to wit;

a) The data subject has given consent to the processing of his/her personal data for one or more specific purposes;
b) 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;
c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
d) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
e) 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
f) Processing is done in the controller's legitimate interest.

In the absence of all of the above-mentioned grounds, there would be no lawful or legal basis for processing and any processing carried out thereto, would be deemed a violation of the provision of the data protection laws in Nigeria. In the case of *Olumide Babalola v Soko Lending Company Ltd*,[8] where

[5]Ibid.
[6]Section 24 (1) (a) of The Nigeria Data Protection Act, 2023.
[7]Zhivka Mateeva Stoyanova, Principles Of Personal Data Protection, Audit 2 (2020), Cild 28, s?h. 95-104 (PDF) Principles of personal data protection (researchgate.net) accessed 16May2023.
[8]Suit No: LD/13031MFHR/2022, High Court of Lagos, Per Justice E. OAshade.

a digital lending company sent an unsolicited Whatsapp message to a no-customer informing him about the indebtedness of a customer unknown to the receiver and further instructing the latter to advise the debtor to pay up his debt, the court held that the sender of unsolicited Whatsapp messages lack lawful basis to send such to a non-customer.

European Union[9] and Court of Europe[10] data protection law**s** also require personal data to be processed lawfully.[11] Accordingly, lawful processing requires the consent of the data subject or another legitimate ground provided in the data protection legislation. *Article* 6 (1) of the GDPR includes five lawful grounds for processing, in addition to consent, i.e., when processing personal data is necessary for the performance of a contract, for the performance of a task carried out in the exercise of public authority, for compliance with a legal obligation, for the purpose of the legitimate interests of the controller or third parties, or if necessary to protect the vital interests of the data subject.

Fairness of Processing: Fairness is also a relatively broad principle, which requires that any processing of personal data must be fair towards the individual whose personal data are concerned, and avoid being unduly detrimental, unexpected, misleading, or deceptive.[12] It deals with the ethics of data protection and requires personal data to be processed in line with the reasonable expectations of the data subject and devoid of adverse effects. The principles require controllers to balance the interests and legitimate expectations of data subjects by ensuring that such processing activities do not negatively impact vulnerable data subjects.[13] The whole essence of the principle of fairness is that the controller should give data subjects enough information about the processing activities and also should be able to demonstrate compliance. Processing activities must not be performed in secret and data subjects should be aware of potential risks. Controllers must act in a way which promptly complies with the wishes of the data subject, especially where his or her consent forms the legal basis for the data processing.[14] In the case of *K.H. & Ors v Slovakia*,[15] where women of Roma ethnic origin was treated in two hospitals in eastern Slovakia during their pregnancies and deliveries. None of them subsequently conceived a child again despite repeated attempts. Upon request, they were prohibited from making copies (but only permitted to make excerpts) of their medical records principally to protect the relevant information from abuse. The European Court of Human Right[16] failed to see how the applicants, who had in any event been given access to their entire medical files, could have abused information concerning themselves. Moreover, the risk of such abuse could have been prevented by means other than denying copies of the files to the applicants, such as by limiting the range of persons entitled to access the files. The state (who prohibited making copies of the record) failed to show the existence of sufficiently compelling reasons to deny the applicants effective access to information concerning their health. The Court concluded that there had been a violation of *Article* 8.

In assessing whether personal data is processed fairly, it is important to consider the interest of those affected data subjects both as a group and individually. For instance, if the information is processed fairly with regard to most of the people it relates to but unfairly with regard to one individual, it will still be regarded as an unfair processing. It is important to note that in some circumstances, personal

[9] Hereinafter referred to as EU.
[10] Hereinafter referred to as CoE
[11] Modernised Convention 108, Article. 5 (3); General Data Protection Regulation, Article. 5 (1) (a).
[12] An Coimisiun Um Chosaint Sonrai, Quick Guide to the Principles of Data Protection <https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf> Accessed 23rd August, 2023.
[13] Lee. A Bygrave, Data Protection Law: Approaching its Rationale, Logic and Limits, (Kluwer International, New York, 2022)110.
[14] European Union Agency for Fundamental Rights, Handbook on European Data Protection Law (Imprimerie Centrale in Luxembourg, 2018) [2018 edn] 118.
[15] ECtHR, K.H. and Others v. Slovakia, No. 32881/04, 28 April 2009.
[16] Hereinafter, referred to as ECtHR.

data may be used in a way that will impact an individual negatively without being unfair.[17]
Transparency of Processing: Transparency is a particularly important principle of data protection within the data protection laws, with various related rights and obligations seeking to ensure that processing of personal data is clear and transparent to individuals and regulators.[18] The principle of transparency requires that any information and communication relating to the processing of their personal data in a format that is concise, easily accessible, easy to understand, and in clear and plain language. This principle has been held to apply even when data controllers are public authorities.[19] This should be done before personal data are collected and subsequently whenever changes to the processing operation are made.

Where it is not clear to a natural person as to how his or her personal data is being processed and the extent of the processing activities, then the controller has breached the principle of transparency. Processing will not be regarded as transparent if for instance, the privacy notice is too long or laced with complex or technical words and sentences or drafted with a tiny font as to cause fatigue reading. Specific rules regarding transparency obligations are found in *Article*s 12, 13, and 14 GDPR, including details on the specific types of information which must be provided to data subjects, and the manner in which it must be provided. In order to be transparent, controllers must ensure the means of conveying information is the most appropriate for their platform and target audience. In *Haralambi v Romania*,[20] the applicant was only granted access to the information held on him by the secret service organisation five years after his request The ECtHR reiterated that individuals who were the subject of personal files held by public authorities had a vital interest in being able to access them. The ECtHR considered that neither the quantity of the files transmitted nor shortcomings in the archive system justified a delay of five years in granting the applicant's request for access to his files. The authorities had not provided the applicant with an effective and accessible procedure to enable him to obtain access to his personal files within a reasonable time. The Court concluded that there had been a violation of *Article* 8 of the ECHR.

2. PURPOSE LIMITATION: The principle of purpose limitation is one of the fundamental principles of data protection laws. It is strongly connected with transparency, predictability and user control: if the purpose of processing is sufficiently specific and clear, individuals know what to expect, and transparency and legal certainty are enhanced. At the same time, clear delineation of the purpose is important to enable data subjects to effectively exercise their rights, such as the right to object to processing.[21] This principle provides that data controllers and processors must only process persona data to achieve the particular purpose for which the personal data was collected and not use it for another purpose unless such further purpose is compatible with the original purpose.[22] It is therefore important for the purpose of complying with this principle for the controller to identify the specific purpose for which the personal data is intended to be processed and to restrict the processing activities with purpose. The processing of personal data for undefined and/or unlimited purposes is thus unlawful. The processing of personal data without a certain purpose, just based on the consideration they may be useful sometime in the future, is also not lawful. The legitimacy of processing personal data will depend on the purpose of the processing, which must be explicit, specified and legitimate.[23]

[17] The Privacy Academy, Certified Associateship Course Handbook, (2023) 39.
[18] An Coimisiun Um Chosaint Sonrai, Quick Guide to the Principles of Data Protection. Ibid.
[19] Judgment of the CJEU of 1 October 2015 in case C201-/14, Smaranda Bara and others v National Health Insurance House and others, paragraphs 28-46 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0201 accessed 18 May 2023.
[20] ECtHR, Haralambie v. Romania, No. 21737/03, 27 October 2009.
[21] Article 29 Working Party (2013), Opinion 3/2013 on purpose limitation, WP 203, 2 April 2013.
[22] Section 24 (1)(b) Nigeria Data Protection Act, 2023.
[23] European Union Agency for Fundamental Rights, Handbook on European Data Protection Law. Ibid 122-123.
[24] Ibid.

The principle of purpose limitation bears an affinity with lawfulness as a basis for processing personal data. Where it is found that the data controller or processor has gone beyond the purpose for which data was collected, any processing done beyond that purpose limitation will violate this principle. Every new purpose for processing data which is not compatible with the original one must have its own particular legal basis and cannot rely on the fact that the data were initially acquired or processed for another legitimate purpose. In turn, legitimate processing is limited to its initially specified purpose and any new purpose of processing will require a separate new legal basis. For instance, disclosure of personal data to third parties for a new purpose will have to be carefully considered, as such disclosure will likely need an additional legal basis, distinct from the one for collecting the data.[24] In the case of *Data Protection Commission v Doolin & Ors,*[25] it was held by the Irish Court of Appeal that the use of CCTV footages in the disciplinary process of an employee was unlawful as the employer's CCTV policy confirmed that CCTV footage was only collected and processed for the specific purpose of security. As such, the employee could not have reasonably expected that the footage would be used to monitor his performance. Thus, this difference in purpose was in contravention of the law.

The Nigeria data protection law permits that a controller in some instance can engage in further or secondary processing of personal data and such instance include:

a) Where the further processing is compatible with the original purpose or
b) Where the further processing is incompatible, and the controller relies on the lawful bases of consent or legal obligation. Then consent must be freshly obtained based on further purpose.
c) Where the further processing is solely for the purpose of scientific research, historically research or for statistical purposes in the public interest.

If the controller intends to rely on any of these foregoing conditions for secondary processing, the controller must mandatorily inform the data subject about the secondary processing prior to undertaking such processing activities, as well as of his or her (data subject) rights, such as the right to object.

The General Data Protection Regulation and Modernised Convention 108 declare that the "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" is a priori considered compatible with the initial purpose.[26] However, appropriate safeguards such as the anonymisation, encryption or pseudonymisation of the data, and restriction of access to the data, must be put in place when further processing personal data.[27] The General Data Protection Regulation adds that "[w]here the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes"[28]

3. DATA MINIMISATION: The law is that personal data must be accurate throughout processing and every reasonable step must be taken to ensure that. This principle requires that controllers only collect and process personal data that are adequate, relevant, without prejudice to the

[25][2022] IECA 117.

[26]General Data Protection Regulation, Article. 5 (1) (b); Modernised Convention 108, Article. 5 (4) (b). An example of such national provisions is the Austrian Data Protection Act (Datenschutzgesetz), Federal Law Gazette I No. 165/1999, para. 46.

[27] General Data Protection Regulation Article. 6 (4); Modernised Convention 108, Article. 5 (4) (b); Explanatory Report of Modernised Convention 108, para. 50.

[28] General Data Protection Regulation, Recital 50.

dignity of human person and limited to what is necessary for the purposes for which they are processed. The principle of data minimization deals with the requirement of data adequacy. This essentially means that data controllers should collect the minimum amount of data they require for their intended processing operation; they should never collect unnecessary personal data. This principle complements in particular, the principle of purpose limitation, but also supports compliance with the range of data protection principle.[29] The principle of data minimization is hinged on two pronged factors of necessity and proportionality. The personal data collected must be necessary and proportionate to the purpose and not more or less.

Necessity: By necessity, processing of personal data must not only be relevant but also necessary or suitable for achieving the aim of the processing activity. When determining the necessity of processing personal data, the controller needs to take into account if there exist alternative less intrusive measures and whether any interference with data protection right arises from the processing in question.[30]

Proportionality: Proportionality on the other hand refers to the amount of personal data collected to achieve a purpose and the accuracy of the personal data. The amount of personal data required to accomplish a processing purpose must not be excessive.

The GDPR does not define what amount of personal data is 'adequate, relevant and limited'. This will have to be assessed by controllers depending on the circumstances of their intended processing operations. Controllers should also periodically review the amount and nature of personal data which they process, ensuring it remains adequate, relevant, and necessary, including by deleting data which no longer fulfil these criteria. In the case of *Digital Rights Ireland*, the Court of Justice of the European Union[31] considered the validity of the Data Retention Directive, which aimed to harmonise national provisions for retaining personal data generated or processed by publicly available electronic communications services or networks for their possible transmission to competent authorities to fight serious crime, such as organised crime and terrorism.
Data minimization does not mean a ban on the collection of certain data, but only that the data controller must have a justification for their collection or otherwise processing. Although this principle may seem like a hindrance in the businesses of data controllers/processors, it actually serves both the interests of the data subject and the data controller.

4. DATA ACCURACY: The law is that personal data must be accurate throughout processing and every reasonable step must be taken to ensure this.[32] This principle requires that a data controllers ensure personal data are accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[33] Controllers should take every reasonable step to ensure that personal data which are inaccurate are erased or rectified without delay, having regard to the purposes for which they are processed.

The provision of the GDPR on the principle of accuracy is much more elaborate than in NDPA[34]. From the GDPR provision, it can be seen that data accuracy forms the underlying principle for a data subject's right to erasure and rectification. This is in order to maintain the quality of the personal data.

[29] An Coimisiun Um Chosaint Sonrai, Quick Guide to the Principles of Data Protection. Ibid.

[30] CJEU Joined cases C-92/09 and C-93/09 Volker und Markus Shecke & Anor v Land Hessen. <https://eur-ex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092> accessed 17 May 2023.

[31] Hereinafter referred to as CJEU.

[32] Alexender Asuquo, The Principles of Nigeria Data Protection Law. Ibid.

[33] Article. 5 (1)(d) of the GDPR.

[34] Section 24 (e) of the NDPA, 2023.

CJEU in *Rijkeboer's case*[35] considered the Dutch national's request to receive information from the local administration of the city of Amsterdam on the identity of the persons to whom the records on him held by the local authority had been communicated in the two preceding years, and also on the content of the disclosed data. The CJEU stated that the "right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients." The CJEU then referred to the preamble of the Data Protection Directive, which states that data subjects must enjoy the right of access to their personal data in order to be able to check that the data are correct.[36]
Thus, data controllers are obligated to provide easy access to personal data in order to demand erasure or rectification, and to also act upon that demand in a timeous manner. In general, the reasonable steps controllers are required to take to ensure the accuracy of personal data will depend on the circumstances and in particular on the nature of the personal data and of the processing. Controllers need to also keep in mind their obligations in relation to data subjects' right to rectification – to have inaccurate personal data rectified, or completed if it is incomplete.[37]

5. STORAGE LIMITATION: This principle activates the question of how long data may be stored by the data controller which cannot be indefinitely, thereby placing a legal limit on how long data can remain in the data controller's database. Controllers must hold personal data, in a form which permits the identification of individuals, for no longer than is necessary for the purposes for which the personal data are processed.[38] *Section* 24 (1)(d) of the NDPA modelled after the GDPR and *Article* 5 (4)(e) of the Modernised Convention 108 provides that personal data shall be stored only for the period within which it is reasonably needed. The data must therefore be erased or anonymised when those purposes have been served. To this end, "time limits should be established by the controller for erasure or for a periodic review" to make sure that the data are kept for no longer than is necessary. In *Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (NIMC)*[40] where a company temporarily moved about one third of its user's personal details to a text database after a flaw had emerged in the operation of the server holding the main database, it was held that *Article* 5(1) (e) of Regulation 2016/679 must be interpreted as meaning that the principle of storage limitation laid down in that provision precludes the storage by the controller, in a database set up for the purpose of testing and correcting errors, and necessary for carrying out those tests and correcting those errors.

Personal data may be stored for longer periods where the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with the GDPR, and as long as there are appropriate technical and organizational measures to safeguard the rights and freedoms of the individual. In *S. and Marper,* the ECtHR concluded that the core principles of the relevant instruments of the Council of Europe, and the law and practice of the other Contracting Parties, required data retention to be proportionate in relation to the purpose of collection and limited in time, particularly in the police sector. The court ruled that indefinite retention of the fingerprints, cell samples and DNA profiles of the two applicants was disproportionate and unnecessary in a democratic society, considering that the criminal proceedings against both applicants had been terminated by an acquittal and a discontinuance, respectively. [41]

[35] CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 7 May 2009.
[36] Former Recital 41, Preamble to Directive 95/46/EC.
[37] Alexender Asuquo, The Principles of Nigeria Data Protection Law. Ibid
[38] Ibid.
[39] Article. 5 (1)(e) of the GDPR.
[40] Unreported Suit No:AB/83/2020, delivered on the 15th July, 2020 by Hon Justice A.A. Akinyemi J.
[41] ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 4 December 2008; see also, for example: ECtHR, M.M. v. the United Kingdom, No. 24029/07, 13 November 2012.

The time limitation for storing personal data only applies to data kept in a form which permits identification of data subjects. Lawful storage of data which are no longer needed could, therefore, be archived by anonymising data. Modernised Convention 108 also permits exceptions to the principle of storage limitation, on the condition that they are provided by law, respect the essence of fundamental rights and freedoms, and are necessary and proportionate for pursuing a limited number of legitimate aims. These include, among others, protecting national security, investigating and prosecuting criminal offences, carrying out criminal penalties, protecting the data subject and protecting the rights and fundamental freedoms of others.

Indefinite data retention is not only an infringement of the rights of an individual but a risk for those processing it. Failure to limit the period for which data is stored increases security risks and raises concerns that it could be used for new purposes merely because it is still available and accessible. There are risks that, if data is outdated, it could lead to poor decision-making processes which could have severe implications.[42]

6. DATA SECURITY/INTEGRITY AND CONFIDENTIALITY: This principle is concerned with the security and secrecy of personal data. The principle require that personal data must be processed by controllers only in a manner that ensures the appropriate level of security and confidentiality for the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. To achieve this end, controllers must utilise appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data.[43] Controllers must ensure that their security measures adequately protect against accidental or deliberate harm, loss, or dissemination of the personal data they process. These security measures should cover not only cybersecurity but also physical and organisational security measures. Organisations must also routinely check that their security measures are up-to-date and effective.[44] By *Article* 2.1 (1)(d) of the NDPR, personal data must be secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements. The duty to protect personal data in line with this principle is so enormous on the controller/processor that the law places the duty of care on the data controller or processor.[45] GDPR which is similarly worded goes further to state that the controller and the processor should take into account "the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" when implementing such measures.[46] Depending on the specific circumstances of each case, appropriate technical and organisational measures could include, for example, pseudonymising and encrypting personal data and/or regularly testing and evaluating the effectiveness of the measures to ensure that data processing is secure.[47]

This principle is one of the touchstones of data protection as it goes to the very root of privacy of individuals. The law therefore requires data controllers to safeguard data by ensuring to put in place strong firewall to protect computerized data and ensuring that every form of personal data is well secured from unauthorised access, theft, manipulations and destruction. This is because the risks and dangers that unauthorized access to personal data poses to data subjects can be very destructive.[48]

---

[42] Alexender Asuquo, The Principles of Nigeria Data Protection Law. Ibid.

[43] Section 24 (2) of the Nigeria Data Protection Act, 2023.

[44] An Coimisiun Um Chosaint Sonrai, Quick Guide to the Principles of Data Protection. Ibid.

[45] See Section 24 (3) of the NDPA and Article. 2.1 (2) of the NDPR.

[46] Article. 32 (1) of the General Data Protection Regulation.

[47] Ibid.

[48] The Privacy Academy, Certified Associateship Course Handbook, (2023) 47.

In cases where a personal data breach takes place, both Modernised Convention 108 and the GDPR require the controller to notify the competent supervisory authority of the breach with the risks for rights and freedoms of individuals without undue delay.[49] A similar communication obligation to the data subject exists when the personal data breach is likely to result in a high risk to his or her rights and freedoms.[50] Communication of such breaches to the data subjects must be in clear and plain language[51]

While data controllers and processors are expected to put in place measures to prevent unauthorized access to personal data of their data subjects, they are equally obliged to implement appropriate technical and organization measures to ensure a level of security appropriate to the risk of processing such personal data. Specifically, anyone involved in data processing or the control of data ought to develop security measures to protect data; such measures may include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.[52]

7. ACCOUNTABILITY: The principle of accountability is a new principle of data protection law, which specifically sets out that controllers are responsible for, and must be able to demonstrate compliance with, the other principles of data protection. This means that controllers need to ensure they comply with the principles, but also have appropriate processes and records in place to demonstrate compliance. The principle essentially saddles a controller with the responsibility to demonstrate its compliance with its obligations under relevant data protection laws. The NDPR which has a similar provision with the NDPA[53] provides that;

(2) anyone who is entrusted with personal data of a data subject or who is in possession of the personal data of a data subject owes a duty of care to the said data subject;

(3) Anyone who is entrusted with Personal Data of a Data Subject or who is in possession of the Personal Data of a Data Subject shall be accountable for his acts and omissions in respect of data processing, and in accordance with the principles contained in this Regulation."[54]

There are two key points in the accountability principle. The data controller owes a duty of care to the data subjects and that the data controller shall be held accountable for his acts in respect of data processing. Although, it is not only the controller that may handle personal data during the whole processing (for example, when the controller engages a processor), but since the controller is the one that data subjects entrust with their personal data, he holds a duty of care to the data subjects. Hence, controller must ensure that the processors process the personal data he provides within the limits of the law.[55]

Appointing a data protection officer (DPO) who will carry out data protection impact assessments (DPIAs), where required, and ensuring that they are properly involved in all issues relating to data protection, maintaining records of processing activities, drafting clear contracts with processors acting on the controller's behalf, where appropriate, are just some of the tools which can assist controllers in complying with the principle of accountability.[56] Ultimately, the principle of accountability reiterates that the data controller is the party most responsible for NDPR compliance. It also means that if something goes wrong, the data controller shall be held accountable.[57]

---

[49] Modernised Convention 108, Article. 7 (2); General Data Protection Regulation, Article. 33 (1).

[50] Ibid. Article. 34 (1).

[51] Article. 34 (2) General Data Protection Regulation.

[52] Article. 2.6 Nigeria Data Protection Regulation, 2019.

[53] Section 24 (3) of the Nigeria Data Protection Act.[54] Article. 2.1 (2) & (3).

[55] The Privacy Academy, Certified Associateship Course Handbook, (2023) 50.

[56] An Coimisiun Um Chosaint Sonrai, Quick Guide to the Principles of Data Protection. Ibid.

[57] Ibid.

The GDPR and Modernised Convention 108 set out that the controller is responsible for, and must be able to demonstrate compliance with, the personal data processing principles.[58] To this end, the controller must implement appropriate technical and organisational measures.[59] Even though the accountability principle in *Article* 5 (2) of the GDPR is only directed towards controllers, processors are also expected to be accountable, given that they have to comply with several obligations and that they are closely connected to accountability,[60] this is also the case with the NDPA.

EU and CoE data protection laws also determine that the controller is responsible for, and should be able to ensure, compliance with all other of the data protection principles.[61] The *Article* 29 Working Party points out that "the type of procedures and mechanisms would vary according to the risks represented by the processing and the nature of the data.[62]

CONCLUSION

Nigeria data protection laws[63] have made significant stride forward in securing personal data and aligning the nation with global privacy standards. As a critical framework for safeguarding personal data in Nigeria, NDPA represents a significant milestone in the country's commitment to privacy and digital security. By setting clear guidelines, the NDPA reinforces individual fundament rights to privacy, supports trust in Nigeria's digital ecosystem, encourages responsible data handling across both public and private sectors and lays the groundwork for both domestic and international/cross-border data data exchange.

However, while this progress has been made, the effectiveness of the NDPA will ultimately depend on the ability of the regulatory bodies[64] to enforce compliance of data protection laws, the public's understanding of their rights, and the adaptability of the law to keep pace with technological evolution. The underfunding or zero funding of the NPDC need to be urgently visited and the seemingly exploitative license fee of Data Protection Compliance Organizations need to be reviewed. Continued focus and improvements are essential and concerted unbiased efforts need to be employed in the implementation of data protections principles and laws Nigeria.

RECOMMENDATIONS

1. **Strengthen Enforcement and Accountability Mechanisms**: Concerted and unbiased efforts should be made to provide Nigeria Data Protection Commission and any other regulatory body or supportive regulatory body, with adequate working resources, skilled personnel, and technological tools for the protection of personal data. This will enable adequate training/awareness, effective monitoring, enforcement of compliance, and swift responses to data breaches. Establishing clear consequences for non-compliance will further reinforce organisational accountability and deter misuse of data.

2. **Increase Public Awareness and Education**: To maximize the impact of the NDPA, targeted public awareness campaigns are essential. Such campaigns could focus on educating citizens about their data rights, highlighting how they can seek redress for violations, and helping organizations understand their legal obligations. Collaborations with educational institutions, NGOs, and technology inclined companies can broaden outreach and make privacy knowledge more accessible to all citizens, particularly in rural and underserved communities.

[58] Article. 5 (2) of the General Data Protection Regulation; Modernised Convention 108, Article. 10 (1).

[59] Article. 24 of the General Data Protection Regulation.

[60] European Union Agency for Fundamental Rights, Handbook on European Data Protection Law. Ibid. 135.

[61] Article. 5 (2) of the General Data Protection Regulation; Modernised Convention 108, Article. 10 (1).

[62] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010, para. 12.

[63] Specifically, the Nigeria Data Protection Act (NDPA) 2023 and Nigeria Data Protection Regulation (NDPR) 2019.

[64] Nigeria Data Protection Commission and Data Protection Compliance Organizations.

3. **Institutionalize Regular Reviews of the NDPA**: Given there is constant and rapid advancement of digital technology, it is important that the NDPA remains flexible and responsive to new changes and challenges. Setting up a periodic review process, perhaps every three to five years, would allow for updates that reflect shifts in global privacy practices, address emerging threats like AI driven surveillance and also incorporate public feedback to enhance the NDPA's relevance.

4. **Support Innovation with Privacy by Design**: Businesses and government institutions should be encouraged to embed privacy principles in the early stages of system and product development. Privacy by design initiative would not only enhance data security but also foster public confidence in digital services. Incentive such as digital certifications or tax breaks could motivate organizations to adopt these privacy-e practices proactively.