GRIFFITH COLLEGE DUBLIN

LLM Dissertation Submission Cover Sheet

Student name:	**Chimfulumnanya Anita Nwafor**
Student number:	**3098602**
Dissertation title:	**Nigerian NDPA vs European Union GDPR: Comparing Data Subject Rights and Privacy Protection**
Supervisor's name:	**Dr Busani Moyo**
Supervisor's signature:	**Dr Busani**

Plagiarism disclaimer:

I understand that plagiarism is a serious offence and have read and understand the college's policy on plagiarism and that my dissertation will be checked for plagiarism through TURNITIN. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this dissertation, or if I have knowingly allowed others to plagiarise my work in this way.

I hereby certify that this dissertation is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the dissertation has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.

Signature of student: **Anita** **Date:** **09/08/2024**

Note to LLM students: You **MUST** submit TWO HARD-BOUND COPIES + A COPY ON MOODLE. You MUST retain the receipt issued to you as proof of submission.

FOR OFFICE USE ONLY:

No. of copies received (please tick):	2 x hard-bound	_____
Confirmation from student that soft copy submitted on Moodle:	Yes	_____
Date:		_____
Received by:	**Name:**	_____
	Signature:	_____

NIGERIAN NDPA VS EUROPEAN UNION GDPR: COMPARING DATA SUBJECT RIGHTS AND PRIVACY PROTECTION

RESEARCH DISSERTATION PRESENTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF LL.M INTERNATIONAL HUMAN RIGHTS LAW

LAW SCHOOL, GRIFFITH COLLEGE DUBLIN

CHIMFULUMNANYA ANITA NWAFOR

2024

CADIDATE DECLARATION

Candidate Name: Chimfulumnanya Anita Nwafor

I certify that the dissertation entitled Nigerian NDPA vs GDPR: Comparing data subject rights and privacy protection, submitted for the degree of LL.M in International Human Rights Law, is the result of my own work and that where reference is made to the work of others, due acknowledgement is given.

Candidates Signature: Anita

Date: 6/08/2024

Supervisor Name: Dr Busani Moyo

Supervisor Signature: Dr Busani

Date: 09/08/2024

ACKNOWLEDGEMENTS

I am profoundly grateful to Griffith College Dublin for the incredible opportunity to present this work and for being a steadfast guide throughout my LLM journey. I extend my heartfelt thanks to my supervisor, Dr Busani Moyo, for his insightful guidance and unwavering support during my research. Lastly, I am deeply appreciative of my lecturers and academic advisor, Dr Ruhi Anand, for her invaluable moral support and encouragement to me and my classmates throughout our course. Lastly, I acknowledge my classmates for their camaraderie, collaboration, and shared dedication, which have enriched this journey.

DEDICATION

I dedicate this work to God Almighty, whose boundless grace and wisdom have guided me through every step. To my beloved parents and siblings, whose unwavering support and encouragement have been my foundation. To my exceptional boss at Local Solicitor, whose invaluable mentorship has shaped my professional growth. And finally, to my wonderful partner Obi, whose steadfast love and inspiration have been my constant companion.

Table of Content

LIST OF ABBREVIATIONS

AEPD: Agencia Española de Protección de Datos

CNIL: Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)

CJEU: Court of Justice of the European Union

GDPR: General Data Protection Regulation

DPO: Data Protection Officer

EU: European Union

ITU: International Telecommunication Union

NIN: National Identification Number

NDPA: Nigerian Data Protection Act

NDPR: Nigerian Data Protection Regulation

NITDA: National Information Technology Development Agency

SMEs: Small and Medium-sized Enterprises

UNCTAD: United Nations Conference on Trade and Development

ABSTRACT

In an era marked by rapid digital transformation, the protection of data subject rights and privacy has become a critical issue globally. This thesis undertakes a doctrinal comparative analysis of the data subject rights found in the Nigerian Data Protection Act (NDPA) and the European Union's General Data Protection Regulation (GDPR), together with an examination of its approaches to privacy protection. The study aims to elucidate the adequacy of these legal frameworks in safeguarding personal data and ensuring privacy. The research begins by providing a background on the evolution of data protection laws, highlighting significant cases such as *Digital Rights Lawyers Initiative & 2 Others v. National Identity Management Commission & 1 Other* which exemplified recent data privacy issues in Nigeria. The thesis examines the specific legal provisions of the data subject rights together with the enforcement provisions found in NDPA and GDPR, which identifies both similarities and divergences influenced by their distinct legal, social, and economic contexts. A critical part of the study involves analysing the enforcement mechanisms of both regulations to determine if the right to privacy is adequately adhered to. The thesis also delves into the cultural, social, and economic factors impacting the implementation of these laws in Nigeria compared to GDPR-compliant regions. Key findings from the comparative analysis reveal that while the GDPR provides a more stringent and comprehensive framework for data protection, the NDPA represents a significant step towards enhancing data privacy in Nigeria. The study identifies areas where the NDPA could benefit from adopting elements of the GDPR, particularly in strengthening enforcement mechanisms by adopting a decentralised approach and ensuring broader rights for data subjects are provided for. On the other hand, the GDPR can emulate the broader provision of the NDPA on the right to data portability. The thesis concludes with a summary of key findings from the comparative analysis and recommendations for policymakers to restructure the provision of data subject rights and enforcement mechanism in the NDPA. Further recommendation is made for policy makers to review the right to data portability found in the GDPR. This work also suggests strategies for overcoming implementation challenges, emphasizing the need for awareness and better enforcement structures in data privacy. This research contributes to the broader discourse on data privacy by offering insights into the adequacy of data protection laws within the Nigerian and European Union frameworks, serving as a foundation for future comparative studies in this domain.

CHAPTER 1

INTRODUCTION

This chapter deals with an introduction to data privacy issues in Nigeria and the need for a comparison of the Nigerian Data Protection Act with the European Union's General Data Protection Regulation (GDPR). The functionality of a right cannot be adequately addressed without a further look into its enforcement mechanisms and factors that hinder its implementation within the jurisdiction it applies. This chapter discusses these points together with a literature review. This chapter is concluded by and identification of the gap in knowledge and the sole essence of putting forth this dissertation.

1.1 Background to the study

In a time of unparalleled data growth and pervasive digital connectedness, privacy rights protection has become essential in present day. As people navigate a world that is becoming more and more digital, worries about data security and privacy have led governments and regulatory agencies all over the world to pass strong laws designed to protect personal data. For instance, in Nigeria, there have been several occurrences of breach of the right to privacy.[1] One recent example of this is the case of *Digital Rights Lawyers Initiative & 2 Others v. National Identity Management Commission & 1 Other*.[2] The plaintiffs challenged the mandatory requirement for individuals to provide their National Identification Number (NIN) for accessing telecommunications services.[3] They argued that this mandatory linkage infringed on individuals' right to privacy, as enshrined in the Nigerian Constitution and other relevant laws.[4] The plaintiffs contended that the collection and storage of biometric data, as

[1] Agbakoba O, 'Privacy Rights and Data Protection in Nigeria: Challenges and Prospects' (2022) 66(2) Journal of African Law, 245-267.
[2] *Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission & 1 Other* [2020] Suit No AB/83/2020.
[3] *Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission & 1 Other* [2020] Suit No. AB/83/2020. Para 10
[4] *Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission & 1 Other* [2020] Suit No. AB/83/2020. Para 12

required by NIMC for the issuance of NIN, violated their right to privacy.[5] They argued that the mandatory nature of the NIN for telecommunications services effectively forced individuals to surrender their biometric data without their explicit consent.[6] The plaintiffs sought a declaration that the actions of NIMC and the requirement to link NIN to telecommunications services were unconstitutional and a breach of their right to privacy.[7] The Federal High Court ruled in favour of the defendants, NIMC and the Attorney General of the Federation. It was held that the requirement to link NIN to telecommunications services was justified in the interest of national security and public interest.[8] It ruled that while the right to privacy is fundamental, it is not absolute and can be lawfully restricted in certain circumstances, such as national security and crime prevention.[9] The court further found that the collection of biometric data and the mandatory linkage of NIN to telecommunications services were necessary measures to combat crime, enhance national security, and ensure proper identification of individuals. With these circumstances, it can be argued that the decision of the court is justifiable because it was geared toward national security and public interest. It can also be argued that the court's decision is justifiable because it supports the general rule that for every law, there is an exception. However, there is still a loop because it entails that the rights of data subject are not adequately protected and thereby falling short of the protection of the right to privacy.

The Nigerian Data Protection Act (NPDA) is a law that is designed to protect the privacy of personal data and regulate its processing among other things. An analysis of this law is important because it would evaluate if a comparison would contribute to balancing privacy protection with economic growth and innovation, national security, and public interest. This is exemplified in section 26 and 34 of the Act. Section 26 of the NDPA provides for consent of the data subject before their data can be collated and processed.[10] On the other hand, section 34 deals with right of access.[11] This provision ensures that data subjects have control over their personal data while also allowing data controllers to collect and process data for various

[5] *Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission & 1 Other* [2020] Suit No. AB/83/2020. Para 18
[6] *Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission & 1 Other* [2020] Suit No. AB/83/2020.
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid.*
[10] Nigerian Data Protection Act 2023, s 26.
[11] Nigerian Data Protection Act 2023 s 34(1)(a).

purposes[12]. In other words, section 26 allows data subject to give their permission before their data is processed while section 34 permits data subjects to access their data. Section 26 goes further to grant the data subject to right to withdraw this consent at any stage, however, a withdrawal of consent shall not affect processing that has been done prior to withdrawal.[13] This strikes a balance between privacy protection and national security, public interest, and business activities in collecting and processing personal data which promote economic growth and innovation. Another example is the provision for data controllers to transfer personal data outside of Nigeria only if there are adequate safeguards in place to protect the data.[14] This provision allows for international data transfers which are necessary for economic growth and innovation while also ensuring that data subjects' privacy rights are protected[15].

In addition to the provisions in the NPDA in relation to the rights of data subjects, the Nigerian judiciary has also played a role in enforcing privacy rights while still maintaining regulatory requirements. For example, in the case of *Nwabueze v. Diamond Bank,*[16] where Nwabueze opened and operated a bank account with Diamond Bank. Nwabueze discovered that certain amounts were being deducted from his account without his authorization. Upon inquiry, he was dissatisfied with the bank's explanation and decided to take legal action against the bank, alleging breach of contract and unauthorized deductions. The court found in favour of Nwabueze, holding that Diamond Bank had indeed breached its contractual obligations by making unauthorized deductions from the plaintiff's account.[17] The court awarded damages to Nwabueze for the financial loss he suffered due to the bank's actions. The court also held that the bank had a duty to protect the customer's privacy rights and could not use the data for any other purpose.[18] This case is discussed because it shows the positive efforts of the Nigerian courts to uphold the right to privacy. However, as highlighted in the Digital Lawyers Initiative case, which was decided the same year as the case of Nwabueze, the ruling of the court

[12] Nigerian Data Protection Act 2023, s 34(1)(a)(i).
[13] Nigerian Data Protection Act 2023 s 26.
[14] Nigerian Data Protection Act 2023, s 41(1)(a).
[15] Nigerian Data Protection Act, 2023, s 41
[16] *Nwabueze v Diamond Bank* [2020] 3 NWLR 193.
[17] *Ibid.*
[18] *Ibid.*

was against the plaintiff, but this is not so in the case of Nwabueze. This only proffer an imbalance in the court system in upholding right to privacy and therefore the reason for comparison

1.2 Statement of the problem

The legal problem which this dissertation deals with is the adequacy of the Nigerian Data Protection Act (NPDA) provisions on data subject rights for an effective privacy protection compared to the General Data Protection Regulation (GDPR) of the European Union. This adequacy should be addressed because despite the enactment of the then Nigerian Data Protection Regulation, now replaced by the NDPA of 2023, there are still inconsistencies by the court in upholding adequate right to privacy of data subject. This issue was highlighted in the cases of *Digital Rights Lawyers Initiative & 2 Others v. National Identity Management Commission & 1 Other* and *Nwabueze v. Diamond Bank* as explained above. Here the courts still find difficulty in balancing privacy rights with national security and economic interest.

Also, though there is a similar nature in the provisions of data subject rights between the NDPA and GDPR,[19] yet the GDPR seem to have gained more recognition outside of the European Union than the NDPA, thereby gaining more recognition and upholding right to privacy beyond the European Union.[20] In the introductory pages of the regulations which deals with its scope, the GDPR applies to all European Union citizens and business domiciled in the European Union which deals with data of European Union citizens.[21] On the other hand, the NDPA though having similar provisions only applies to Nigerian citizens domiciled in Nigeria and businesses operating outside Nigeria, but process data of Nigerian citizens domiciled in Nigeria. The act has no provision on processing of data of Nigerian citizens domiciled outside Nigeria. The reason for this illustration is to show that the GDPR, because of its recognition outside of the European Union, has enhanced the adherence of right to

[19] Greenleaf G, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2018) 157 Privacy Laws & Business International Report, 14-18.
[20] *Ibid.*
[21] General Data Protection Regulation [2016] OJ L119/1

privacy while the NDPA seem to cut off the privacy rights of Nigerians domiciled outside of Nigeria.

An in-depth analysis of both laws reveals that the GDPR seem to have a more comprehensive provision of data subject rights than the NDPA.[22] The NDPA merely listed some of these rights without stating how they can be exercised or its limitations. Example is the right to erasure provided for in section 34(1)(v). On the other hand, the case of Max Schrems demonstrates the recognition of the GDPR beyond the EU. In this case, Max Schrems, an Austrian privacy advocate, challenged the validity of the Privacy Shield framework on the grounds that U.S. laws did not offer sufficient protection for EU citizens' data.[23] The CJEU ruled that the Privacy Shield framework was invalid because it did not provide adequate protection against U.S. surveillance practices that could undermine the fundamental rights of EU citizens as guaranteed under the GDPR.[24] The ruling emphasized that for data transfers to be lawful under GDPR, the recipient country must offer a level of protection equivalent to that of the EU.

1.3 Objectives of the study

1. Introduction of the study's context, objectives, and review existing literature on data protection laws and privacy rights in Nigeria and the European Union.
2. Examine data subject rights and enforcement under the NDPA implementation.
3. Examine data subject rights and enforcement under the GDPR and their implementation challenges.
4. Compare data subject rights and enforcement mechanisms between the NDPA and GDPR, highlighting their implementation challenges.
5. Summarize key findings, provide recommendations, and draw conclusions based on the comparison of data subject rights and enforcement between the NDPA and GDPR

1.4 Research Methodology

In this study, a dual methodological approach is employed, integrating both doctrinal and comparative methods, with a specific focus on comparative doctrinal analysis. The doctrinal

[22] Ibrahim L, 'A Comparative Analysis of Data Protection Frameworks in the EU and Nigeria: Key Issues and Challenges' (2020) 10(1) International Data Privacy Law, 29-44.
[23]Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECJ 1.
[24] *Ibid.*

method involves a detailed examination of legal texts, statutes, and case law to elucidate the principles and rules governing the subject matter. This foundational analysis provides a comprehensive understanding of the legal framework and its theoretical underpinnings. Complementing this, the comparative doctrinal method is utilized to juxtapose the legislative provisions of different jurisdictions. By systematically comparing the content and adequacy of these provisions, the study aims to identify potential gaps in the existing legal frameworks. Additionally, the research examines how cultural, social, and economic factors influence the functionality of these regulations. This holistic approach not only highlights the strengths and weaknesses of each jurisdiction's approach (if any), but also offers insights into the broader contextual factors that impact the effectiveness of legal solutions, thereby contributing to the development of more nuanced and effective regulatory frameworks.

1.5 Scope and Limitation

The scope of this work solely focuses firstly on rights of data subjects who are persons whose data are in the possession of another person called a data controller. These data subject rights are provided for both the NDPA and GDPR and the scope of this work does not extend to other areas which deals with data protection in general. The GDPR applies to any organization processing the personal data of European Union citizens, regardless of where the organization is located.[25] The Nigerian NPDA, on the other hand, only applies to organizations that are registered in Nigeria or that process the personal data of Nigerian citizens based in Nigeria by data controllers outside of Nigeria.[26] The GDPR has extraterritorial applicability, meaning that it applies to any organization processing the personal data of European Union citizens, regardless of where the organization is located. The Nigerian NPDA does not have the same level of extraterritorial applicability because it falls short of the provision for processing personal data of Nigerians that are domiciled outside of Nigeria.[27] Therefore, it seems the GDPR has a broader scope than the NDPA, for this reason this scope of this work secondly, surrounds Nigerian data subjects domiciled in Nigeria, and EU data subjects domiciled all over the world. Thirdly, the scope of this work extends to the enforcement mechanisms provided in both laws to ensure these data subject rights are protected thereby upholding the right to privacy.

[25] General Data Protection Regulation [2016] OJ L119/1
[26] Nigeria Data Protection Act 2023, s 2(2).
[27] Nigerian Data Protection Act 2023 pt 1.

The scope of this work further extends to the rights of data subjects provided for in the legislation and their enforcement mechanisms. However, this work is limited to only 4 rights of interest considering an analysis of each of this right will be dealt with. These rights include Right to access personal data, right to rectification, right to not be subject to automated decision making and right to data portability. This work is further limited to the enforcement mechanisms provided in section 5 and 6 of the NDPA and articles 51, 55, 57 and 70 of the GDPR for the purpose of the analysis of the enforcement mechanisms to achieve the aim of this work on privacy protection. In relation to this discussion on factors that affect proper implementation of the enforcement framework, this work is limited to only the cultural, Economic, and social factors in the discussion section on factors influencing the adherence of the provisions for data subject rights. Also, regarding the discussion on factors influencing enforcement of this right, this work will be limited to the use of Ireland, being a European Union jurisdiction to examine these factors, while also using Nigeria being the jurisdiction on which the NDPA applies.

1.6 Significance of the study

The significance of this study lies in its comprehensive analysis of data subject rights and privacy protection under both legislations. By comparing these two frameworks, this study aims to contribute to several key areas. The comparative analysis highlights the areas where the NDPA can benefit from the GDPR and vice versa. This can inform ongoing and future policy developments in Nigeria and the EU, helping to promote best practices for data privacy. It offers recommendations for businesses and organizations on how to effectively implement these rights, thus improving compliance and reducing the risk of data breaches and misuse. The research contributes to the broader academic discourse on data protection by providing insights into the functioning of data subject rights within different legal and cultural contexts. With data flows becoming increasingly global, this study underscores the importance of international cooperation in data protection.

1.7 Research Questions

The central research question is ‘How adequate is the data subject rights provided for in the NDPA and GDPR when compared by their provisions and privacy protection mechanism together with implementation challenges associated with each?

There are 5 questions that flow from the central research question, and they include:

a. What are the primary contexts, objectives, and legal frameworks of the NDPA and GDPR regarding data protection and privacy rights?
b. Are data subject rights defined and enforced under the NDPA together with its implementation challenges enough to uphold right to privacy?
c. Are data subject rights defined and enforced under the GDPR together with its implementation challenges enough to uphold right to privacy?
d. Does a comparison of the data subject rights and enforcement mechanisms between the NDPA and GDPR together with its implementation challenges uphold right to privacy in both regions?
e. What are the key findings from comparing the NDPA and GDPR in terms of data subject rights and privacy protection, and what recommendations can be made to address the identified challenges to uphold right to privacy?

1.8 Understanding the historical overview of data protection and privacy rights.

In this subheading, this work will proffer a coherent background to the origin of data protection laws in Nigeria and the EU. This work acknowledges that over the years, there has been numerous enactments that deal on data privacy but for the purpose of theme of this dissertation, recourse will only be made to the Nigerian Constitution, The European Chater on Human Rights, and The Nigerian Data Protection regulation.

In a time when data-driven decision-making and digital innovation are dominating, privacy rights protection has become a critical human rights issue in relation to right to privacy as provided for in Article 8[28] of the European Charter on Human Rights (ECHR) and section 37[29] of the Constitution of the Federal Republic of Nigeria (CFRN). There has never been a greater pressing need for strong data privacy laws due to the growing amount of personal information that people reveal online. Legislative frameworks like the above discussed have been designed to protect people's privacy rights and control the processing of personal data. Due to the distinct legal traditions and socio-cultural circumstances of each region, the NPDA and GDPR may initially seem to be two different laws. But a deeper look finds startling similarities and points where these two regulatory frameworks overlap. The foundation of both

[28] European Convention on Human Rights [1950] OJ 1 11
[29] Constitution of the Federal Republic of Nigeria 1999, s 37.

legislation is the understanding that privacy is a basic human right, as recognised by international treaties like the European Convention on Human Rights.[30]

1.8.1 The Constitution of the Federal Republic of Nigeria (CFRN)

The Constitution of the Federal Republic of Nigeria (CFRN)[31] is the supreme legal document that enshrines the fundamental rights of individuals in sections 33-46 within Nigeria, but the focus of this work is on section 37. Among these rights is the right to privacy which is cornerstone for section 34 of the Nigerian Data Protection Act (NPDA). By embedding privacy within the constitutional framework, Nigeria ensures that personal data protection is not only a legislative matter but also a constitutional imperative. Section 37 of the CFRN explicitly guarantees the right to privacy.[32] It declares: "The privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected.[33] " The Nigerian judiciary has consistently upheld Section 37 of the CFRN, reinforcing its application and significance through various landmark cases. For instance, in *Ojukwu v. Governor of Lagos State*[34] where a dispute arose over the eviction of Ojukwu from a property in Lagos. Ojukwu claimed he was unlawfully evicted from a government-owned property, while the Lagos State Government asserted that he was occupying the property illegally.[35] The Supreme Court addressed the forceful eviction and ruled that this action was unconstitutional, emphasizing that the privacy of citizens' homes is protected under Section 37. This case shows the judiciary's role in safeguarding the constitutional right to privacy against unauthorized intrusions by the state.[36] Similarly, in *Gani Fawehinmi v. Nigerian Bar Association,*[37] the court dealt with the Nigerian Bar Association's attempt to inspect lawyers' files without their consent. The court found such inspections to be a violation of the right to privacy contained in Section 37 of the constitution, thereby reinforcing the principle that personal correspondence and communications are inviolable without due process.[38] In another significant case, *Alhaji Mujahid Dokubo-Asari v. Federal Republic of Nigeria,*[39] the court examined the detention of

[30] European Convention on Human Rights [1950] OJ 1 11.
[31] Section 37.
[32] Section 37.
[33] *Ibid*.
[34] *Ojukwu v Governor of Lagos State* [1986] 1 NWLR (FHC) Pt 18, 621.
[35] *Ibid.*
[36] *Ibid.*
[37] *Gani Fawehinmi v Nigerian Bar Association* [1989] 2 NWLR (HC) Pt 105, 558.
[38] *Ibid.*
[39] *Alhaji Mujahid Dokubo-Asari v Federal Republic of Nigeria* [2007] 30 WRN (SC) 1.

Dokubo-Asari, a Niger Delta activist, whose correspondence, and communication were monitored without a warrant.[40] The court ruled that this monitoring infringed upon his constitutional right to privacy, as protected by Section 37. These cases collectively underscore the judiciary's commitment to upholding the right to privacy as enshrined in the CFRN[41]. Given these case studies, it is safe to say that the interpretation of the section given by the Nigerian courts underscores the comprehensive scope of privacy rights in Nigeria, extending protections across various forms of personal communication and the privacy of one's home. By enshrining the right to privacy at the constitutional level, Nigeria establishes a legal foundation for the protection of individual privacy against undue interference in Nigeria.

The NPDA draws its legitimacy from the constitutional guarantee of privacy, ensuring that its provisions are not merely statutory but also enjoy constitutional backing.[42] This constitutional foundation enhances the NPDA's enforceability, providing a strong legal basis for protecting personal data as stated in its objectives in Part 1 of the Act.[43] Furthermore, the NPDA builds upon the broad protections offered by Section 37 to provide detailed and specific safeguards for data privacy. This includes protections against unauthorized data collection, processing, and transfer, thereby addressing modern privacy concerns in the digital age.[44]

1.8.2 European Convention on Human Rights

Article 8 of the European Convention on Human Rights (ECHR) enshrines the right to respect for private and family life, home, and correspondence. It states:

"1. Everyone has the right to respect for his private and family life, his home, and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"[45].

[40] *Ibid.*
[41] *Ibid.*
[42] Nigerian Data Protection Act 2023, s 1.
[43] Nigerian Data Protection Act 2023, pt 1 s 1.
[44] Nigerian Data Protection Act 2023, Pt V.
[45] European Convention on Human Rights [1950] OJ 1 11.

This article has been interpreted and applied in numerous cases by the European Court of Human Rights (ECtHR). Here are some notable cases and themes in the interpretation of Article 8 regarding the right to privacy:

a. Private Life: The ECtHR has interpreted the notion of "private life" broadly to encompass various aspects of an individual's personal autonomy, including sexual orientation, identity, personal autonomy, and personal development. In cases such as *Dudgeon v. the United Kingdom (1981) and Pretty v. the United Kingdom,*[46] the Court affirmed that private life includes the right to live as one chooses and to develop one's identity.[47]

b. Family Life: The concept of "family life" extends beyond the traditional nuclear family to include relationships formed outside of marriage or blood ties.[48] The Court has recognized the importance of family relationships and has protected rights such as parental rights[49] and the rights of unmarried couples.[50]

c. Home: Article 8 protects the right to respect for one's home, which includes not only the physical dwelling but also the right to control who enters and what activities occur within it.[51] The Court has held that interference with the home, such as through unauthorized surveillance or forced evictions, must be justified and proportionate.[52]

d. Correspondence: This aspect of Article 8 protects communications, both physical and electronic, from unjustified interference by public authorities. The Court has emphasized the importance of safeguards against arbitrary surveillance and interception of communications.[53]

e. Balancing of Rights: Article 8(2) allows for limitations on the right to privacy when such limitations are necessary in a democratic society and pursue legitimate aims. The ECtHR employs a balancing test to assess whether interferences with privacy are proportionate to the legitimate aims pursued. Factors such as the nature of the interference, the importance of the legitimate aim, and the safeguards in place are considered.[54] These cases and interpretations

[46] *Dudgeon v United Kingdom* (1981) 4 EHRR 149. *Pretty v United Kingdom* (2002) 35 EHRR 1.
[47] *Ibid.*
[48] *Johnston and Others v Ireland* (1986) 9 EHRR 203.
[49] *Keegan v Ireland* (1994) 18 EHRR 342.
[50] *Johnston and Others v Ireland* (1986) 9 EHRR 203.
[51] *Chapman v United Kingdom* (2001) 33 EHRR 399.
[52] *Connors v United Kingdom* (2004) 40 EHRR 189.
[53] *Liberty and Others v United Kingdom* (2008) 48 EHRR 1.
[54] *Marckx v Belgium* (1979) 2 EHRR 330. *S and Marper v United Kingdom* (2008) 48 EHRR 50.

demonstrate the evolving understanding of the right to privacy under Article 8 of the ECHR, balancing individual rights with societal interests and the needs of a democratic society.

1.8.3 The Nigerian Data Protection Regulation: The Nigerian Data Protection Regulation (NDPR) was enacted in 2019 to deal with data privacy issues that was rampant years ago. However, as time went on, the regulation was found to be defective because of its inadequacies in data subject right. Because of a scarcity in case laws on the regulation, this work will discuss what different scholars has put forth on the lapses of the regulation. For example, Iwu-James et al.[55] compared the data subject rights provisions of the then NPDR and the GDPR. They noted that while the NPDR provides data subjects with the right to access, correct, and erase their personal data, it falls short of the GDPR's right to data portability.[56] The authors argued that this is a significant gap in the NPDR's data subject rights provisions, as it limits the ability of data subjects to control their personal data.[57]

Furthermore, Adediran et al[58] examined the privacy protection provisions of the NPDR and the GDPR. They noted that while both frameworks require data controllers to obtain the consent of data subjects before collecting or processing their personal data, the GDPR is more stringent in its requirements.[59] They also argued that the GDPR's requirement for a Data Protection Officer and the conduct of Data Protection Impact Assessments are important privacy protection measures that were lacking in the NPDR of 2019. Olugbenga-Bello and other scholars examined the enforcement of the NPDR and the GDPR. They noted that while the NPDR had had limited enforcement and case laws, the GDPR has been subject to numerous cases and has had a significant impact on the data protection landscape in the EU.[60] They argued that the lack of enforcement and case law under the NPDR is a significant challenge to its effectiveness as a regulatory framework for data protection in Nigeria. It is safe to say that while the GDPR has had significant impact and enforcement in the EU, the lack of enforcement and case law under the NPDR of 2019 is a significant challenge to its adequacy as a regulatory framework for data protection in Nigeria. Though the numbers are

[55] Iwu-James J, James T, and Iwu C, 'A Comparative Analysis of Data Protection Frameworks in Nigeria and the EU' (2021) 5(2) Journal of International Data Privacy Law 45.
[56] *Ibid.*
[57] *Ibid.*
[58]Adediran O, Oluwaseun A, and Eze S, 'The Evolving Landscape of Data Protection in Nigeria: Challenges and Opportunities' (2021) 7(1) African Journal of Law and Technology 89.
[59] *Ibid*.
[60] Olugbenga-Bello A, Akande T, and Eniola A, 'Data Protection Laws in Nigeria and the GDPR: A Comparative Study' (2021) 3(4) Nigerian Journal of Data Protection and Privacy 112.

still low in the current NDPA of 2023, these works help to provide some insight into its inception.

1.9 Review of literature on the Nigerian NPDA and GDPR and Gaps in Knowledge

Having rendered a foundation to the birth of the Nigerian Data Protection Act, this literature review will highlight several research which has put forward a discussion on the GDPR and NDPA. Before delving in, it is important to point out that the NDPA is relatively a new enactment that came into force in June 2023. Whereas, the GDPR has been in force since 2018. This implies that there could potentially be limited research in the NDPA, but this might not be the case under the GDPR.

In a paper by Ba-balola O, an analysis of the NDPA 2023 through the lens of legal transplant theory was rendered.[61] The paper talked about the NDPA within a historical and comparative framework, exploring the adoption of GDPR-like standards in Nigeria. Ba-balola emphasized the necessity of adapting these standards to Nigeria's unique cultural, legal, and operational contexts, noting significant challenges such as institutional capacity, public awareness, and financial resources.[62] His findings highlight the potential of the NDPA to boost international trust and position Nigeria as a regional leader in data protection. However, the paper identified practical challenges, including enforcement difficulties and the need for extensive public education.[63] Ba-balola recommended tailoring the NDPA to Nigerian realities, enhancing regulatory bodies' capacity, and implementing iterative legal reforms based on empirical feedback. Although the analysis seems comprehensive, it would benefit from more specific case studies to illustrate successful legal transplants. This article is highly relevant because the author provides a theoretical framework for understanding how and why the NDPA 2023 mirrors the GDPR, essential for a comparative analysis of data subject rights. By situating the NDPA within the context of legal transplants, the article explains the motivations and implications behind adopting GDPR-like standards in Nigeria, essential for analysing these laws' practical function.[64] Ba-balola highlighted similarities in data subject rights between the GDPR and NDPA, such as access, rectification, erasure, and data portability.[65]

---

[61] Ba-balola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) British Journal of Cyber Criminology 3, 1.
[62] Ba-balola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) British Journal of Cyber Criminology 3, 5-7.
[63] *Ibid.*
[64] Ba-balola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) British Journal of Cyber Criminology 3, 8.
[65] *Ibid.*

The emphasis on adapting these rights to the Nigerian context aids in discussing the practical challenges of protecting these rights in Nigeria compared to the EU. The analysis of institutional challenges in Nigeria provides insights into the practical enforcement of these rights, contrasting with the EU's framework.[66] He offered recommendations for contextual adjustments and iterative reforms in the NDPA as a basis for suggesting improvements, aligning better with GDPR standards while addressing local challenges.[67] Ba-balola's call for stakeholder engagement is relevant for discussing regulatory improvements through feedback. The use of legal transplant theory adds depth to the comparative analysis, emphasizing the broader implications of adopting a foreign legal framework. In conclusion, Ba-balola's article is a valuable resource for comparing data subject rights and privacy protection under the GDPR and NDPA.

The GDPR has been extensively studied due to its comprehensive and stringent approach to data protection within the EU. Its influence extends globally, setting a benchmark for data privacy standards.[68] Studies indicate that data subject rights are essential in enhancing privacy protection. By data subjects I mean persons whose personal data are held by another person. For instance, Voigt and von dem Bussche argue that the rights to access, rectification, erasure, and data portability empower individuals to manage their personal information proactively.[69] These rights, embedded in GDPR, enable individuals to request information about data processing, correct inaccuracies, delete unnecessary data, and transfer data between service providers, thus fostering transparency and accountability in data processing.[70] However, implementing these rights poses significant challenges. According to Gonzalez and Lamek, organizations face difficulties in complying with the stringent requirements of GDPR, particularly in the areas of data erasure and portability.[71] The technical and administrative burdens of locating and modifying data across complex IT

[66] Ba-balola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) British Journal of Cyber Criminology 3, 1.
[66] Ba-balola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) British Journal of Cyber Criminology 3, 5-7.
[67] *Ibid.*
[68] Greenleaf G, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2018) 157 Privacy Laws & Business International Report, 157. Goddard, M 'The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact' (2017) 59(6) International Journal of Market Research, 703-705.
[69] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edn, Sringer 2017).
[70] *Ibid.*
[71] Gonzalez, G., & Lamek, M, 'GDPR Implementation Challenges' (2018) 2(3) Journal of Data Protection & Privacy 203-218.

systems can be overwhelming, especially for small and medium-sized enterprises.[72] Moreover, the need for better verification processes to prevent fraudulent data access requests adds another layer of complexity.[73] Another critical piece is by Adeyemi I., which explores the enforcement mechanisms of the GDPR and their potential application within the Nigerian context under the NDPA.[74] Adeyemi's research delves into the practical challenges faced by European regulators and how these experiences could inform the enforcement strategies of Nigeria's data protection authorities.[75] The study highlights the GDPR's robust enforcement framework, including the roles of supervisory authorities and the mechanisms for imposing penalties. Adeyemi suggests that while Nigeria can benefit from adopting similar enforcement strategies, there are significant hurdles, such as limited regulatory capacity and potential resistance from local businesses.[76] The paper proposes a phased approach to enforcement, starting with high-impact sectors and gradually expanding as regulatory capacity improves. Adeyemi's recommendations include strengthening institutional frameworks and fostering international cooperation to enhance enforcement effectiveness.[77] Lastly, Ojo T's work offers a detailed comparative examination of the NDPA and GDPR. Ojo evaluates how the NDPA reflects GDPR principles, noting similarities in data subject rights, such as access and erasure.[78] However, the study highlights key differences, particularly in enforcement and regulatory capacity.[79] The NDPA, while adopting GDPR-inspired principles, faces challenges such as limited public awareness and technological infrastructure. Ojo's analysis underscores the need for Nigeria to adapt GDPR standards to its local context and suggests incremental improvements to bridge the gap between the NDPA and GDPR.[80] This study provides valuable insights into Nigeria's progress and the practical challenges of achieving full GDPR equivalence.[81]

---

[72] *Ibid.*
[73] *Ibid*.
[74] Adeyemi I, 'Enforcement Mechanisms of the GDPR and Their Application in Nigeria's NDPA: Lessons and Challenges' (2024) 12 Nigerian Journal of Law and Technology 45-63.
[75] *Ibid.*
[76] *Ibid.*
[77] *Ibid.*
[78] Ojo T, 'The Nigerian Data Protection Act 2023: A Comparative Analysis with the GDPR' (2023) 18 *African* Journal of Information and Communication Law 23-42.
[79] *Ibid.*
[80] *Ibid.*
[81] *Ibid.*

1.9.1 Gaps in the literature

There is a limited number of comprehensive comparative studies between the GDPR and the NPDA, particularly those focusing on in-dept analysis of the data subject rights and enforcement mechanisms. Furthermore, there is insufficiency in works that dealt with adequacy of these rights and the enforcement mechanisms under the NPDA and GDPR in ensuring adequate protection of privacy. Also, there has not been any work which deeply discussed the detailed provision of data subject rights and how they are exercised in Nigeria and European Union. Lastly, though recognised, the specific ways in which cultural and socio-economic factors influence the effectiveness of data protection laws need further exploration. In this section this work seeks the bridge the gap between how the cultural and socio-economic factors influence the enforcement of the NPDA in Nigeria and how it compares to the GDPR in the EU.

CHAPTER 2

NDPA: LEGAL PROVISIONS, ENFORCEMENT AND IMPLEMENTATION CHALLENGES

INTRODUCTION

The Nigerian Data Protection Act (NPDA) of 2023 serves as the primary legislation for data protection in Nigeria, forming a crucial part of this work. This Act is designed to balance the imperatives of data protection with the need for economic growth, offering comprehensive provisions that empower data subjects with a variety of rights.[82] These rights are fundamental to the overarching theme of data privacy and are critical in an era where data misuse can lead to significant harm. The NPDA outlines several key rights for data subjects, primarily encapsulated in Part VI of the Act. These rights ensure that individuals maintain substantial control over their personal data. This chapter would discuss in detail the six data subject rights of interest which this work is limited to. This chapter would discuss whether the provision describes how these rights should be exercised. Furthermore, a part of this chapter will discuss the enforcement provision that has been put in place to ensure adherence to the right. Lastly, this chapter will discuss the factors within the Nigerian jurisdiction which will aid or impede the implementation of these 6 rights. It is important to point out that because this is a new legislation, which was enacted in June 2023, there are no records of reported cases on the act. In addition, there are little or no articles which ineptly analysed this right as this is one of the gaps in knowledge which this work seeks to cover.

2.1 Examination of select provisions in the Nigerian NPDA for the safeguard of Data subject rights

This section aims to examine four rights of data subject which this work is limited to under the NDPA. These rights include right to access personal data, right to rectify personal data, right related to automated decision making and lastly right to data portability. These rights will be examined in-depth with reference to its content.

[82] Nigerian Data Protection Act 2023, pt 1.

2.1.1 Right to Access Personal Data

The right of Access is a right provided for in section 34 of the NDPA. This right is a fundamental aspect of data protection laws, ensuring that data subjects can obtain information about their personal data being processed by data controllers or processors.[83] Data subjects are entitled to receive confirmation from the data controller or processor on the storage or processing of their personal data.[84] This clause contains wordings which demonstrate that people be informed about the existence of data processing operations pertaining to their personal information. This subsection infers three main points. First, it ensures that individuals are aware of the existence of data processing activities involving their personal data. Second, for data subjects to exercise additional Act rights, such the right to rectify or erase their data, they must first obtain confirmation that their data is being processed. Data subjects cannot properly exercise their rights if they do not know whether their data is being processed. Third, this clause makes data controllers and processors responsible for their data handling procedures by requiring them to verify data processing operations. It guarantees that they keep precise records of all data processing operations and are ready to provide data subjects with this information.

Once it is confirmed that personal data is being processed, the data subject has the right to know the purposes for which their data is being processed.[85] This will help individuals understand the reasons behind the collection and use of their data, ensuring that it is not being used for purposes beyond what was originally intended or consented to. By informing data subjects of the purpose for processing of their data, it shows the existence of transparency and trust and thereby preventing misuse of personal data. Knowing the purposes of data processing helps ensure that data is not used beyond what was originally intended or consented to. The clause further provides that the data controller must disclose the categories of personal data being processed.[86] This means that the data subject should be informed about the specific types of data being handled, such as contact information, financial details, health records, etc. Knowing the categories of data helps the data subject understand the scope of data processing. The data subject also has the right to know the recipients or categories of recipients to whom their personal data has been or will be disclosed.[87] This part ensures that

[83] Nigerian Data Protection Act 2023, s 34.
[84] Nigerian Data Protection Act 2023, s 34(1)(a).
[85] Nigerian Data Protection Act 2023, s 34(1)(a)(i).
[86] Nigerian Data Protection Act 2023, s 34(1)(a)(ii).
[87] Nigerian Data Protection Act 2023, s 34(1)(a)(iii).

data subjects are aware of where their data is being transferred and who has access to it. Lastly, when at all practicable, the data controller should let the data subject know how long their personal information will be kept on file.[88] The criteria used to identify that timeframe should be provided if the precise period cannot be specified.[89] This makes it easier for people to understand how long their data will be kept and why, as well. Also, the section also provides that data subjects must also be informed of their right to request rectification or erasure of personal data, the restriction of processing, or to object to such processing, along with the right to lodge a complaint with a supervisory authority. If the personal data is not collected directly from the data subject, any available information about its source must also be communicated. During research, it appears that section 34(1)(a) did not make any provision regarding how the right to access can be exercised. By this I mean, there is no stipulated provision showing how the data subjects can exercise this right. There is no section which talks about a body which stipulates how this right can be exercise. Example, whether it should be made in writing or not, and who should it be addressed to.

2.1.2 Right to Rectification Personal Data

The right to rectification is explicitly provided for in the NDPA in section 34(1)(a)(v), together with other rights and is not isolated in a separate section. Instead, it is embedded within the broader framework of data subject rights in section 34. Specifically, it was mentioned in section 34(1)(a)(v) together with other rights like right to reassure. Right to rectification implies that data subjects have the right to request that any inaccurate or incomplete personal data be corrected or updated. This provision ensures that individuals can maintain control over their personal information and ensures that data controllers are held accountable for the accuracy of the data they process. This is buttressed in section 24(e) of the Act. The NDPA outlines the procedure for exercising the right to rectification. However, the act does not grant the data subject the right to request for a rectification of data but rather places obligation on the data controller to make the necessary corrections without undue delay.[90] The Act also requires that, where appropriate, the data controller must inform any third parties to whom the data has been disclosed about the rectification.[91] A closer look at this provision reveals that much power is placed on the data controller rather than the data subjects. This could give room for an abuse of power. In essence, a data controller could

[88] Nigerian Data Protection Act 2023, s 34(1)(a)(iv).
[89] *Ibid.*
[90] Nigerian Data Protection Act 2023, s 24(e).
[91] *Ibid*.

decide that when he deems appropriate to inform the data subjects. While the NDPA provides a clear framework for the right to rectification, there is currently limited reported case law on its interpretation by Nigerian courts. This is likely due to the recent enactment of the Act.

2.1.3 Right to Data Portability

The right to data portability, as outlined in the NDPA in section 38, is a significant right in the aspect of data privacy laws. It empowers data subjects by granting them control over their personal data, allowing them to receive and transmit their data in a structured, commonly used, and machine-readable format.[92] Subsection (2) of the section explicitly details the entitlements of the data subject under this right. It ensures that data subjects can receive their personal data without undue delay from a data controller.[93] This provision is essential as it mandates timely access to personal data, which is critical for individuals who may need their data for various purposes, such as switching service providers or verifying information. Furthermore, the right to transmit personal data to another data controller without any hindrance facilitates seamless data transfer, thereby promoting competition and innovation among service providers.[94] The clause allowing direct transmission of data between controllers, where technically possible, further simplifies the process for data subjects, reducing the burden on them to manage the transfer themselves. Subsection (3) grants the Commission the authority to prescribe the circumstances and conditions under which the right to data portability can be exercised.[95] This provision suggest that this right can only be exercised at the discretion of the Nigerian Data Protection Commission. Just like the right to rectification, there is no stipulated way in which this right can be exercised. Additionally, it empowers the Commission to impose obligations on data controllers and processors regarding costs and timing,[96] which is crucial for ensuring that the right to data portability is not only accessible but also practical and fair for all parties involved. However, this still gives room for abuse of power by putting the sole responsibility on the data controller to determine factors such as timing and costs. The right to data portability is relatively new and has not been extensively litigated, therefore there is little or no reported case laws by the Nigerian courts on the interpretation of this right.

[92] Nigerian Data Protection Act 2023, s 38.
[93] Nigerian Data Protection Act 2023, s 38(2).
[94] *Ibid*.
[95] Nigerian Data Protection Act 2023, s 38(3).
[96] *Ibid.*

2.1.4 Rights Related to Automated Decision-Making

This right is enshrined in Section 37(1) of the NDPA, which aims to protect individuals from decisions that could significantly affect them without human intervention.[97] Automated decisions can have profound implications, such as affecting creditworthiness, employment opportunities, or access to services. Therefore, this right ensures that individuals are not unfairly disadvantaged by decisions made solely by algorithms or automated systems.[98] Section 37(2) outlines specific exceptions to this right. These exceptions include situations where the automated decision is necessary for entering into or performing a contract between the data subject and the data controller, where it is authorized by law, or where the data subject has given explicit consent.[99] These exceptions recognize that there are circumstances where automated decisions are practical and necessary. For instance, in the context of a contract, automated processing might be essential for accuracy. Section 37(3) further elaborates on the safeguards that must be implemented by the data controller. These safeguards include the right of the data subject to obtain human intervention, express their point of view, and contest the decision.[100] This provision ensures that even when automated decisions are made, there is a mechanism for human oversight and intervention. It acknowledges the limitations of automated systems and the need for human judgment in complex or nuanced situations. By allowing data subjects to contest decisions, the law provides a means for individuals to challenge potentially unfair or incorrect outcomes.

A close look at this section, together with the other rights explained above, shows that major obligation is places on the data controller as duties to be done towards the data subject to clearly portray the true meaning of the act. It can be argued that while this is a good step to ensure that data subjects are not subjected to decision by automated means, the exceptions could potentially be abused because power was placed on the data controller excessively. What this mean is that, like other rights described above, the NDPA fall short of provision on how this right should be exercised. The primary focus of the tis work is on data subject rights to note if it has carried on the true meaning of right to privacy in article 8 of the charter and section 37 of the Nigerian Constitution. A right which is provided in principle on paper,

[97] Nigerian Data Protection Act 2023, s 37(1).
[97] *Ibid.*
[98] *Ibid.*
[99] Nigerian Data Protection Act 2023, s 37(2).
[100] Nigerian Data Protection Act 2023, s 37(3).

without stipulating how it should be exercised but placing this power on one superior body cannot be deemed a proper right to privacy.

2.2 Analysis of the Enforcement Mechanisms

The enforcement mechanisms for data subject rights are contained in section 5 and 6 of the Act, which contains its functions and powers. This subheading will provide an analysis of these enforcement mechanism, only to the extent that this work is limited to. Section 5 delineates the functions of the Commission, which include regulating the deployment of technological and organizational measures to enhance personal data protection.[101] By accrediting, licensing, and registering suitable persons to provide data protection compliance services, the Commission ensures that only qualified entities handle sensitive personal data. Additionally, the registration of data controllers and processors of major importance helps maintain a comprehensive database of key players in the data processing ecosystem. Promoting awareness among data controllers and processors about their obligations under the Act is another crucial function of the Commission.[102] This includes educating the public about personal data protection rights and the associated risks. By receiving complaints related to violations of the Act, the Commission acts as a watchdog, ensuring that any breaches are promptly addressed.[103] The ability to acquire, sell, let, lease, or dispose of property enables the Commission to manage its resources effectively to fulfil its mandate.[104] Furthermore, the act mentioned that the NDPC helps foster the development of personal data protection technologies, in accordance with recognised international best practices and applicable international law.[105] One fact that could be pointed out in these functions is that the sole power for administering the act in its entirety lies solely on the NDPC. In addition, proper definition on what the act referred to as "international best practices" is not defined. There is no parameter put forth to show what amounts to best practices in the international sphere. This sums up the observation that the administration, interpretation and enforcement of the act lies solely on the NDPC with no option for checks.

Section 6 grants the Commission extensive powers to enforce the provisions of the Act. These powers include overseeing the implementation of the Act, prescribing fees for data

[101] Nigerian Data Protection Act 2023, s 5.
[102] Nigerian Data Protection Act 2023, s 5(e).
[103] *Ibid.*
[104] Nigerian Data Protection Act 2023, s 5(g).
[105] Nigerian Data Protection Act 2023, s 5(b).

controllers and processors, and issuing regulations, rules, directives, and guidance.[106] The Commission can also prescribe the manner and frequency of compliance returns by major data controllers and processors, ensuring ongoing accountability and transparency. The power to call for information and inspect documents allows the Commission to conduct thorough investigations into any violations of the Act.[107] This is crucial for identifying and addressing non-compliance. The Commission's authority to impose penalties for violations serves as a deterrent against breaches and ensures that data controllers and processors adhere to the legal requirements.[108] By granting the Commission extensive powers to regulate, oversee, and enforce compliance, we can decipher that this legislation seeks to ensure that data subjects' rights are protected as these mechanisms provide a necessary check on the activities of data controllers and processors, fostering a culture of accountability and transparency. However, it can be argued that this promotes a usurpation of power by the NDPA thereby eluding checks and balances in the system.

The case of *Paradigm Initiative Nigeria & Ors v. The Nigerian Communications Commission*[109] is significant in the discussion of enforcement mechanisms because it highlights the judiciary's role in upholding data protection rights. In this case, the plaintiffs challenged the Nigerian Communications Commission (NCC) over its role in surveillance and interception of communications.[110] The plaintiffs argued that the NCC's actions violated the right to privacy and data protection of Nigerian citizens.[111] The court held that the NCC must ensure that its surveillance activities comply with legal standards and safeguard individuals' rights.[112] There are limited cases on the enforcement mechanism of this act, but this case is necessary to show the attitude of Nigerian courts towards the need for privacy protection.

2.3 Factors influencing the implementation of data subject rights.

The effectiveness of the Nigeria Data Protection Act (NDPA) is significantly influenced by several factors, but for the purpose of this work, focus will only be limited to the cultural, social, and economic contexts.

---

[106] Nigerian Data Protection Act 2023, s 6.
[107] *Ibid.*
[108] *Ibid.*
[109] *Paradigm Initiative Nigeria & Ors v. The Nigerian Communications Commission* [2023] 3 NWLR (Pt 1868) 151.
[110] *Ibid.*
[111] *Ibid.*
[112] *Ibid*.

2.3.1 Cultural Factors: In Nigeria, cultural perceptions of privacy often differ significantly from Western conceptions. Privacy is frequently viewed within the context of community and family rather than as an individual right.[113] This communal perspective could possibly complicate the enforcement of data protection laws designed to safeguard individual privacy rights. The communal nature of Nigerian societies means that data sharing within families and communities is common, potentially leading to unintentional breaches of the NDPR.[114] For instance, it is not uncommon for family members to share personal data such as phone numbers, bank account details, or health information without considering it a privacy violation. This practice, while culturally accepted, poses a significant challenge to enforcing data protection regulations that are predicated on the notion of individual consent and autonomy. As a result, there is a need for culturally sensitive awareness campaigns that educate the public on the importance of individual data privacy rights while respecting communal values.[115]

2.3.2 Social Factors: Social factors refer to the societal influence the populace in general has which could affect proper administration and enforcement of data subject rights. Low levels of digital literacy among the general population pose a significant challenge to the effective implementation of the NDPA.[116] Many Nigerians are not fully aware of their privacy rights or how to exercise them.[117] This lack of awareness is evident in the limited number of complaints filed and a general reluctance to challenge organizations that misuse personal data[118]. Efforts to enhance digital literacy and educate the public about data protection rights are important in addressing these social barriers. For example, targeted educational programs and public awareness campaigns can play a vital role in informing citizens about their rights and how to protect their personal data.

2.3.3 Economic Factors: Economic factors here refer to the financial constraints or determinants which impede the administration and enforcement of data subject rights. These considerations include a look into businesses in operation in Nigeria, which deal with large or

---

[113] Adeoye A. Akinsanya and John A. Ayoade, *An Introduction to Political Science in Nigeria* (2nd edn, University Press of America 2013) 138.
[114] Ifeoma Ajunwa, 'The Illusion of Privacy in Social Media: An African Perspective' (2013) 31 Journal of Information, Communication and Ethics in Society 251.
[115] Ajayi, G. O, 'Digital Literacy and the Challenges of Data Protection in Nigeria', (2020) 18(3) Journal of Information, Communication and Ethics in Society 345-360.
[116] Achuonye KA, 'Digital Literacy and Primary Educational System in Nigeria' (2012) 3 Journal of Educational and Social Research 1.
[117] S A Oluwadare and F A Adebesin, 'Data Protection in Nigeria: The Current State and Future Directions' (2022) 12 Journal of Nigerian Law and Technology 45-67.
[118] *Ibid.*

medium sized volume of data of individuals. For many businesses, particularly small and medium-sized enterprises (SMEs), the cost of compliance with the NDPA can be prohibitive.[119] In addition, the world Bank report of 2020 indicated that businesses in Nigeria face significant regulatory complexities and costs.[120] It ranked Nigeria 131st out of 190 economies for ease of doing business, noting that regulatory compliance can be burdensome and costly, particularly for smaller businesses.[121] This supports the idea that data protection regulations, which add another layer of compliance, can be particularly challenging for SMEs. Investing in secure data storage solutions, appointing Data Protection Officers (DPOs), and implementing comprehensive data protection measures require resources that many SMEs may not have. This economic constraint could possibly lead to partial compliance or outright neglect of data protection obligations. The high cost of compliance is a significant barrier for many Nigerian businesses.[122] Many SMEs struggle to allocate the necessary resources for data protection, leading to inadequate security measures and increased vulnerability to data breaches.[123]

2.4 Discussion on the Impact of These Factors on the Right to Privacy in Nigeria

The implementation and enforcement of the NDPA, and consequently the right to privacy contained in the act are influenced by various factors. This subheading will discuss how the cultural, social, and economic contexts discussed in 2.3 above positively or negatively impact the right to privacy.

Culturally, the communal nature of Nigerian societies can pose challenges to the enforcement of data protection laws. Privacy is often viewed within the context of community and family, rather than as an individual right.[124] This perspective could complicate the enforcement of laws designed to safeguard individual privacy rights. Therefore, there is a need for culturally sensitive awareness campaigns that educate the public on the importance of individual data privacy rights while respecting communal values. Socially, low levels of digital literacy

[119] Nigerian Economic Summit Group, 'The State of Data Protection in Nigeria' (NESG Research Reports, 2021) 45-60.
[120] World Bank, 'Doing Business 2020: Comparing Business Regulation in 190 Economies' (2020) World Bank Publications. Oluwole, O., *Data Protection and Privacy in Nigeria: Law and Practice* (University of Lagos Press 2021).
[121]World Bank, 'Doing Business 2020: Comparing Business Regulation in 190 Economies' (2020) World Bank Publications.
[122] *Ibid.*
[123] *Ibid.*
[124] Adeoye A. Akinsanya and John A. Ayoade, *An Introduction to Political Science in Nigeria* (2nd edn, University Press of America 2013) 138.

among the general population pose a significant challenge to the effective implementation of the NDPA.[125] Many Nigerians are not fully aware of their privacy rights or how to exercise them.[126] This lack of awareness is evident in the limited number of complaints filed and a general reluctance to challenge organizations that misuse personal data[127]. Therefore, targeted educational programs and public awareness campaigns can play a vital role in informing citizens about their rights and how to protect their personal data. Economically, the cost of compliance with the NDPA can be prohibitive for many businesses, particularly small and medium-sized enterprises (SMEs).[128] The high cost of compliance is a significant barrier for many Nigerian businesses.

2.5 CONCLUSION

This chapter has explored the Nigerian Data Protection Act (NDPA) of 2023, focusing on data subject rights, enforcement mechanisms, and implementation challenges. The NDPA offers foundational protections but lacks detailed guidelines for exercising rights such as access and data portability, potentially leading to misuse by data controllers. The Nigerian Data Protection Commission (NDPC) faces transparency and accountability issues despite its extensive powers. Cultural norms, low digital literacy, and economic pressures on SMEs further complicate enforcement. Addressing these challenges through targeted awareness campaigns, public education, and SME support is essential for effective data protection and privacy enhancement.

[125] Achuonye KA, 'Digital Literacy and Primary Educational System in Nigeria' (2012) 3 Journal of Educational and Social Research 1.
[126] *Ibid*.
[127] *Ibid.*
[128] Nigerian Economic Summit Group, 'The State of Data Protection in Nigeria' (NESG Research Reports, 2021) 45-60.

CHAPTER 3

GDPR: LEGAL PROVISIONS, ENFORCEMENT AND IMPLEMENTATION CHALLENGES

INTRODUCTION

The EU General Data Protection Regulation (GDPR) of 2016 is a cornerstone of data protection laws in the European Union. Its relevance extends beyond the European Union, influencing data privacy standards in the European Union and serving as a benchmark for legislation in other countries, including Nigeria's NPDA.[129] This chapter delays with an in-depth analysis of the 6 data subject rights which this work is limited to. It will further discuss whether this regulation provided for how these rights are enforced. Lastly, this chapter will discuss the factors which foster or impede the implementation of these rights. There are several case laws that will be referred to in this analysis of these rights and in the discussion on the enforcement. In this instance, this work will delve into how the courts interpret the provisions on the enforcement mechanisms.

3.1 Examination of specific provisions in the European Union GDPR for the safeguard of data subject rights

This section aims to examine four rights of data subject which this work is limited to under the GDPR. These rights include right to access personal data, right to rectify personal data, right related to automated decision making and lastly right to data portability. These rights will be examined in-depth with reference to its content.

3.1.1 Right to Access of Personal Data

Article 15 of the General Data Protection Regulation (GDPR) confers a fundamental right upon data subjects to access their personal data and obtain essential information regarding its processing.[130] The core of Article 15 lies in its detailed requirements for what information

[129] Ba-balola O, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) British Journal of Cyber Criminology 3, 1.
[130] General Data Protection Regulation [2016] OJ L119/43.

must be provided to data subjects. Initially, it grants data subjects the right to confirm whether personal data concerning them is being processed.[131] This confirmation is the first step towards transparency, enabling individuals to ascertain whether their data is being utilized by a data controller. Once processing is confirmed, the data subject is entitled to access the personal data itself and a suite of pertinent information. This includes the purposes of processing, the categories of personal data involved, and the recipients or categories of recipients to whom the personal data have been or will be disclosed.[132] Significantly, this encompasses any recipients in third countries or international organizations, ensuring that data subjects are informed about cross-border data transfers.[133] Moreover, the provision requires data controllers to disclose the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period.[134] Data subjects must also be informed of their right to request rectification or erasure of personal data, the restriction of processing, or to object to such processing, along with the right to lodge a complaint with a supervisory authority. If the personal data is not collected directly from the data subject, any available information about its source must also be communicated.

In practical terms, the right of access was robustly interpreted in the *British Airways Data Breach Case,*[135] where the UK's Information Commissioner's Office (ICO) fined British Airways £20 million for a data breach that exposed the personal data of approximately 400,000 customers[136]. While this case primarily involved data security, it also touched on the right of access. The ICO's investigation revealed that British Airways failed to provide clear information to data subjects about the breach and did not adequately support individuals in accessing their data in the aftermath[137]. This case emphasized the importance of timely and transparent communication regarding data breaches and the right of data subjects to access information about their personal data, especially when it is compromised. Furthermore, the right of access cannot be fully analysed without considering the case of *Schrems v. Data Protection Commissioner.*[138] This landmark case, adjudicated by the Court of Justice of the European Union (CJEU), underscores the extent of the right to access and its implications for

[131] General Data Protection Regulation [2016] OJ L119/43.
[132] General Data Protection Regulation [2016] OJ L119/43.
[133] General Data Protection Regulation [2016] OJ L119/43.
[134] General Data Protection Regulation [2016] OJ L119/43.
[135] British Airways Data Breach Fines (Information Commissioner's Office, 2020) https://ico.org.uk/about-the-ico/news-and-events/news-articles/british-airways-data-breach-fine/ accessed 8 August 2024.
[136] *Ibid.*
[137] *Ibid.*
[138] *Schrems v Data Protection Commissioner* [2015] C-362/14 ECJ.

data protection. In this case, Max Schrems, an Austrian privacy advocate, sought to exercise his right of access under the GDPR to understand how his data was being processed by Facebook, particularly in relation to its transfer to the United States.[139] The case highlighted the inadequacies in the previous Safe Harbor framework for data transfers between the EU and the US, ultimately leading to its invalidation. The CJEU ruled that data subjects must have the ability to access and understand the processing of their personal data, including any transfers to third countries, to ensure their data is adequately protected.[140]

Exercising the right of access involves the data subject submitting a request to the data controller. Under the GDPR, the data controller must respond without undue delay and at the latest within one month of receiving the request.[141] This period may be extended by two further months if necessary, considering the complexity and number of requests. The data controller is obliged to inform the data subject of any such extension within one month of receiving the request, along with the reasons for the delay. If the data controller decides not to act on the request, they must notify the data subject without delay, at the latest within one month, providing reasons for not acting and information on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.[142] The GDPR in article 15 seem to offer a comprehensive content on what right of access entails. Analysis shows that the regulation further went on to show how this right can be exercised, thereby offering a guide to data subjects on how to exercise their rights contained in articles 15-22.

3.1.2 Right to Rectification of Personal Data

This right allows data subjects to request the correction of inaccurate personal data and the completion of incomplete data concerning them, thus playing a crucial role in maintaining data quality and protecting individual privacy.[143] The provision of Article 16 explicitly states that "the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her"[144]. Furthermore, it allows data subjects to have incomplete personal data completed, including by means of providing a supplementary statement.[145] This right is inherently linked to the principles of data accuracy and integrity, as outlined in Article 5(1)(d) of the GDPR, which mandates that personal data

[139] *Ibid.*
[140] *Ibid.*
[141] General Data Protection Regulation [2016] OJ L119/39.
[142] General Data Protection Regulation [2016] OJ L119/40.
[143] General Data Protection Regulation [2016] OJ L119/43.
[144] *Ibid.*
[145] *Ibid.*

must be accurate and kept up to date.[146] Where data is found to be inaccurate, it must be corrected or erased in line with the data subject's rights under the GDPR.

In terms of evidence and practical application, the case of *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[147] provides a significant judicial interpretation of data rectification within the broader context of data protection rights. While this case is more famously associated with the "right to be forgotten," it also touches upon the rectification of personal data. Mario Costeja González requested that outdated and irrelevant information about his financial troubles be removed from Google's search results.[148] The Court of Justice of the European Union (CJEU) ruled in favour of González, establishing that individuals have the right to request the removal or rectification of personal data that is inaccurate, inadequate, irrelevant, or excessive in relation to the purposes for which they are processed.[149] This decision underscored the broader implications of data accuracy and rectification in protecting personal data. Also, in *NT1 & NT2 v. Google LLC*[150] case, the High Court of England and Wales examined the right to rectification in the context of search engine results.[151] The claimants, NT1 and NT2, sought to have certain outdated and inaccurate information about them removed from Google's search results. The court ruled in Favor of NT2, who was a public figure and had more valid grounds for rectification. However, it rejected NT1's claim, highlighting that the right to rectification also considers the context of the individual's role in public life and the nature of the information[152]. This case underscores the balance between the right to rectify personal data and the public interest in access to information. Furthermore, In *GC and Others v. Facebook Ireland Ltd*[153]*,* the CJEU addressed the right to rectification in the context of social media platforms. The claimants argued that Facebook had not adequately addressed their requests for the removal or correction of personal data that was inaccurate or outdated[154]. The court ruled that data controllers must take appropriate measures to ensure that personal data is accurate and up to date[155]. The case emphasized that the right to rectification is enforceable

[146] General Data Protection Regulation [2016] OJ L119/35.
[147] Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECJ.
[148] *Ibid.*
[149] *Ibid.*
[150] *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB).
[151] *Ibid.*
[152] *Ibid.*
[153] Case C-136/17 *GC and Others v Facebook Ireland Ltd* EU:C: 2019:402.
[154] *Ibid.*
[155] *Ibid.*

and that data controllers must act promptly to address inaccuracies, reflecting the broader principles of data accuracy and protection.

Just like the right to access, the GDPR provides that this right is exercised in accordance with the guidelines provided for in Article 12 of the regulation. This article lists out several provisions with the inclusion of how data subjects can exercise their rights provided in article 15-22 of the regulation. This procedure has been explained in 3.1.1 above.

3.1.3 Right to Data Portability

Article 20 states that data subjects have the right to receive the personal data concerning them, which they have provided to a data controller, in a structured, commonly used, and machine-readable format.[156] Furthermore, they have the right to transmit this data to another data controller without hindrance from the original controller, provided the processing is based on consent or a contract and is carried out by automated means.[157] This provision is intended to ensure that personal data can move freely and efficiently, enhancing the user's ability to manage and switch between service providers. The right to data portability has several important components. Firstly, the data must be provided in a structured, commonly used, and machine-readable format, which ensures that the data can be easily processed by different systems. Secondly, the right applies only to data that the data subject has provided to a controller. This includes data actively given by the data subject (such as name, address, and payment details) and data generated by the subject's activity (such as usage logs and browsing history). Thirdly, the processing of this data must be based on the data subject's consent or a contract, and the processing must be carried out by automated means.

Several case laws practicalize the application of the right to data portability. First, In *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände,*[158] the CJEU focused on the right to data portability in the context of consent and data collection practices.[159] The case involved a challenge to the validity of consent obtained by Planet49 for data processing.[160] The court ruled that for data portability to apply, consent must be valid, and the data must be provided in a machine-readable format.[161] This case highlighted the

[156] General Data Protection Regulation [2016] OJ L119/45.
[157] General Data Protection Regulation [2016] OJ L119/45.
[158] Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und* Verbraucherverbände EU:C:2019:801.
[159] *Ibid.*
[160] *Ibid.*
[161] *Ibid.*

importance of valid consent in the exercise of data portability and reinforced the requirement for data controllers to provide data in an accessible format. Also, in *Schwab v. Facebook Ireland Ltd,*[162] the claimant sought to exercise their right to data portability by requesting their personal data from Facebook. The case revolved around whether Facebook provided the data in a structured, commonly used, and machine-readable format.[163] The court ruled that Facebook complied with the GDPR requirements by providing the data in a suitable format.[164] This case underscored the practical aspects of data portability and the obligation of data controllers to facilitate the transfer of personal data in a manner that allows for easy reuse by the data subject or another data controller. Lastly, in *Nowak v. Data Protection Commissioner.*[165] This case, adjudicated by the Court of Justice of the European Union (CJEU), involved a data subject who requested the transfer of his personal data from one service provider to another.[166] The court ruled in favour of the data subject, affirming that data portability is essential for ensuring that individuals can control and transfer their personal data efficiently.[167] This decision underscored the importance of data portability in the context of digital services. This right is exercised in accordance with the guidelines provided for in article 12 of the GDPR. A close examination of the right to data portability provided for in the GDPR falls short of the cost incurred for the actual transfer or movement of the data on request of the data subject.

3.1.4 Right related to Automated Decision Making

In the age of big data and artificial intelligence, the right not to be subjected to automated decision-making expressed in Article 22 of the GDPR serves as a pillar for individual protection. Article 22 of the GDPR asserts that individuals have the right not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects or similarly significantly affect them.[168] This is intended to protect individuals from decisions made entirely by automated means that could have profound implications on their lives, such as in credit scoring, hiring processes, and insurance underwriting. The provision emphasizes that for this right to apply, the decision must be solely automated, meaning that there is no

[162] Schwab v Facebook Ireland Ltd [2021] EWHC 1058 (QB).
[163] *Ibid.*
[164] *Ibid.*
[165] *Nowak v Data Protection Commissioner* (2017) C-434/16 ECJ.
[166] *Ibid.*
[167] *Ibid.*
[168] General Data Protection Regulation [2016] OJ L119/46.

meaningful human involvement in the process.[169] Additionally, the decision must have legal effects or significantly impact the individual, such as altering their legal status, financial status, employment opportunities, or other critical aspects of their lives.[170] However, the GDPR does provide certain exemptions to this right. Automated decision-making is permissible if it is necessary for entering into or performing a contract between the data subject and a data controller, authorized by Union or Member State law, or based on the data subject's explicit consent.[171] Even within these exceptions, there must be safeguards in place to protect the data subject's rights, including the right to obtain human intervention, express their point of view, and contest the decision.[172] The practical application and enforcement of this right are illustrated by a number of case, First is the case of *Ryneš v. Úřad pro ochranu osobních údajů,*[173]

which dealt with automated decision-making in the context of a parking fine issued by an automated system. Ryneš challenged the legality of the automated decision-making process under Article 22 of the GDPR.[174] The CJEU ruled that automated decisions are permissible if they are based on explicit consent or contractual necessity[175]. However, it stressed that even in such cases, data subjects must have the opportunity for human intervention and the ability to contest the decision[176]. This case reinforced the need for safeguards and transparency in automated decision-making processes. Also, in *Uniqlo Co., Ltd v. Spanish Data Protection Authority,*[177] the CJEU addressed issues related to automated decision-making and profiling. The case involved the use of an automated system by Uniqlo for employee monitoring and decision-making[178]. The court found that the system's use violated the GDPR because it did not provide adequate safeguards for human intervention and did not inform employees about the automated processing of their data[179]. This case highlighted the importance of transparency and the right to human review in automated decision-making processes, reinforcing the

[169] General Data Protection Regulation [2016] OJ L119/46.
[170] General Data Protection Regulation [2016] OJ L119/46.
[171] General Data Protection Regulation [2016] OJ L119/46.
[172] General Data Protection Regulation [2016] OJ L119/46.
[173] Case C-345/17 *Ryneš v Úřad pro ochranu osobních údajů* EU:C: 2017:237
[174] *Ibid.*
[175] *Ibid.*
[176] *Ibid.*
[177] *Uniqlo Co., Ltd v Spanish Data Protection Authority* [2021] EWHC 2156.
[178] *Ibid.*
[179] *Ibid.*

protections under Article 22 of the GDPR. Lastly, the case of the French data protection authority, CNIL, against Futura Internationale in 2018.[180] Futura Internationale used an automated system to manage marketing calls, including a profiling mechanism that categorized individuals based on their socioeconomic status and other criteria.[181] The system made automated decisions about which individuals to target for marketing purposes[182]. CNIL found that Futura Internationale's practices violated the GDPR, as the company had not obtained explicit consent from the individuals for profiling and automated decision-making.[183] Moreover, it failed to inform the data subjects adequately about the processing of their data and their right to object to such processing.[184] This case highlights the necessity for transparency and explicit consent in automated decision-making processes and underscores the importance of providing individuals with clear information about how their data will be used, ensuring they have the means to exercise their rights under the GDPR.

Individuals can exercise their right under Article 22 in several ways. Data controllers are required to inform individuals if their data is being processed by automated means and how such processing will affect them, providing this information in a clear and accessible manner.[185] If automated decision-making is used, individuals have the right to request human intervention in the decision-making process, ensuring that a human reviews and potentially overturns the automated decision if it is deemed unfair or incorrect.[186] Furthermore, individuals can express their concerns about automated decisions and contest the outcome, which is crucial for ensuring fairness and accountability in automated systems. Where automated decision-making is based on consent, individuals must provide explicit and informed consent and can withdraw their consent at any time.[187] Like the NDPA, the right not to be subjected to automated decision making appear to be similar except for the fact that the GDPR has extra provisions which allows the data subject to exercise this right in their own capacity and not just obligations placed on the data controller to safeguard the right.

---

[180] *Commission Nationale de l'Informatique et des Libertés (CNIL), 'Sanction Pronounced Against Futura Internationale'* (27 December 2018) Decision No SAN-2018-011.
[181] *Ibid.*
[182] *Ibid.*
[183] *Ibid.*
[184] *Ibid.*
[185] General Data Protection Regulation [2016] OJ L119/41. General Data Protection Regulation [2016] OJ L119/42.
[186] General Data Protection Regulation [2016] OJ L119/43.
[187] General Data Protection Regulation [2016] OJ L119/43.

3.2 Analysis of Enforcement Mechanisms

The enforcement mechanisms provided for in the GDPR is spread across different articles but for the purpose of this work, attention will only be drawn to articles 51, 57, 58 and 70 of the GDPR. This work focuses only on this section because it deals with enforcement which cover data subject rights and for the fact that these articles can be directly comparted to those of the NDPA in article 5 and 6. These enforcements will be analysed for the purpose of determining if it has checkmated the adherence to data subject rights to uphold right to privacy. An analysis of these enforcement will be done by referring to case laws as evidence for its usage. However, because the enforcement mechanism is not major focus of this work, an in-depth analysis would not be done. However, these mechanisms need to be discussed because this means will enable us find out if the provisions for enforcement of these rights discussed above actually uphold the right to privacy.

Article 51 of the GDPR establishes the supervisory authority, a key body for enforcing the regulation. According to this provision, each Member State must provide for one or more independent public authorities responsible for monitoring the application of the GDPR[188]. These authorities are tasked with protecting the fundamental rights and freedoms of natural persons in relation to processing and facilitating the free flow of personal data within the Union.[189] In cases where more than one supervisory authority is established in a Member State, that Member State must designate the supervisory authority which will represent those authorities in the Board.[190] It must also set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.[191]

Article 57 of the GDPR outlines the tasks of each supervisory authority within its territory. The primary task of the supervisory authority, as per Article 57, is to monitor and enforce the application of the GDPR.[192] This involves promoting public awareness and understanding of the risks, rules, safeguards, and rights in relation to data processing.[193] The supervisory authority also advises national institutions on legislative and administrative measures relating to data protection.[194] Furthermore, it promotes awareness among data controllers and

[188] General Data Protection Regulation [2016] OJ L119/65.
[189] General Data Protection Regulation [2016] OJ L119/65.
[190] General Data Protection Regulation [2016] OJ L119/65.
[191] General Data Protection Regulation [2016] OJ L119/65.
[192] General Data Protection Regulation [2016] OJ L119/68.
[193] General Data Protection Regulation [2016] OJ L119/68.
[194] General Data Protection Regulation [2016] OJ L119/68.

processors of their obligations under the GDPR.[195] The supervisory authority is also tasked with handling complaints lodged by a data subject, or by a body, organization, or association.[196] It investigates the subject matter of the complaint and informs the complainant of the progress and outcome of the investigation.[197] The authority also cooperates with other supervisory authorities to ensure the consistent application and enforcement of the GDPR.[198]

Article 58 of the GDPR provides a comprehensive catalogue of investigative, corrective, and advisory powers placed on the supervisory authority.[199] Investigative powers include ordering the controller and the processor to provide any information required for the performance of its tasks, carrying out investigations in the form of data protection audits, and obtaining access to all personal data and to all information necessary for the performance of its tasks.[200] Corrective powers include issuing warnings and reprimands, ordering compliance with the data subject's requests, imposing a temporary or definitive limitation including a ban on processing, and imposing an administrative fine.[201] Advisory powers include advising the controller in accordance with the prior consultation procedure referred to in Article 36 and issuing opinions to the national parliament, the Member State government, or other institutions and bodies as well as to the public on any issue related to the protection of personal data.[202]

To illustrate the enforcement of Article 58, let's consider the case of Meta (formerly known as Facebook), which was fined €1.2 billion in May 2023.[203] The Irish Data Protection Commission (DPC) imposed this historic fine for transferring personal data of European users to the United States without adequate data protection mechanisms.[204] Another notable case is the €746 million fine issued to Amazon.com Inc. by the Luxembourg National Commission for Data Protection (CNDP) in July 2021.[205] The fine was issued due to a complaint filed by 10,000 people against Amazon through a French privacy rights group, La Quadrature du Net.[206] The CNPD found infringements regarding Amazon's advertising

[195] General Data Protection Regulation [2016] OJ L119/68.
[196] General Data Protection Regulation [2016] OJ L119/68.
[197] General Data Protection Regulation [2016] OJ L119/68.
[198] General Data Protection Regulation [2016] OJ L119/68.
[199] General Data Protection Regulation [2016] OJ L119/69.
[200] General Data Protection Regulation [2016] OJ L119/69.
[201] General Data Protection Regulation [2016] OJ L119/70.
[202] General Data Protection Regulation [2016] OJ L119/70.
[203] Irish Data Protection Commission, 'Decision on Inquiry IN-18-5-7' (31 December 2022).
[204] *Ibid.*
[205] Luxembourg National Commission for Data Protection (CNPD), 'Decision on Amazon.com Inc' (16 July 2021) Decision No 2021-009.
[206] *Ibid.*

targeting system that was carried out without proper consent.[207] These cases demonstrate the commitment of supervisory authorities to uphold data protection regulations and highlight the increasing financial consequences of non-compliance. They also underscore the effectiveness of Article 58 in enforcing the GDPR, thereby ensuring the protection of personal data.

Article 70 of the General Data Protection Regulation (GDPR) delineates the tasks of the European Data Protection Board. The Board's primary responsibility is to ensure the consistent application of the GDPR across the European Union.[208] To this end, the Board can act on its own initiative or at the request of the European Commission.[209] The Board's tasks include monitoring and ensuring the correct application of the GDPR, advising the Commission on any issue related to data protection in the Union, and issuing guidelines and recommendations on various aspects of data protection.[210] These aspects range from procedures for erasing links, copies, or replications of personal data from publicly available communication services, to specifying the criteria and conditions for decisions based on profiling, to establishing the personal data breaches and determining the undue delay for notification of such breaches. The enforcement of Article 70 is evident in the cases discussed above. However, it is important to point out that unlike the total independence accorded to the NDPA, the EDPB cannot only act on its own initiative but also at the request of the European Commission, thereby checking the powers of the EDPB.

3.3 Factors influencing enforcement Mechanisms.

The effectiveness of the General Data Protection Regulation (GDPR) is significantly influenced by several factors, but for the purpose of this work, focus will only be limited to the cultural, social, and economic contexts. However, because the European Union is made of several jurisdiction, attention will only be drawn to Ireland, which will be used as a jurisdictional example in Europe to discuss these factors.

3.3.1 Cultural factors: Ireland's cultural environment, which is firmly anchored in its political, social, and historical settings, has a big impact on how data protection laws defend the rights of data subjects. Karen McCullagh clarified in her work how cultural views influence how legal frameworks are operationalised.[211] In Ireland, the individualistic focus of

[207] *Ibid.*
[208] General Data Protection Regulation [2016] OJ L119/76.
[209] General Data Protection Regulation [2016] OJ L119/77.
[210] General Data Protection Regulation [2016] OJ L119/77.
[211] Karen McCullagh, *Data Protection Law: Approaches to Privacy Governance in the EU and US* (Cambridge University Press 2020).

EU data privacy regulations, like that represented in GDPR, frequently collides with the cultural emphasis on community and collective well-being.[212] This contradiction can be seen in a more collective approach to data privacy, in which the community's needs and values are weighed against everyone's rights.[213] For example, Ireland's long history of local government and public participation encourages everyone to be vigilant about data usage, making sure that the necessary enforcement measures are in place. However, this communal focus might also lead to challenges in prioritizing individual data subject rights, as local cultural norms might implicitly encourage the overlooking of individual grievances in favour of perceived communal benefits.[214]

3.3.2 Social Factors: Digital literacy and attitudes towards technology are also two social elements that have a big impact on GDPR implementation in Ireland. The public is aware of their rights to privacy because of the high levels of digital participation and generally tech-savvy nature of the populace. Greater compliance is made possible by this social climate because people are more inclined to assert their rights and demand accountability from organisations. The paper by John Donovan explores this relationship. According to Donovan's research, greater digital literacy promotes better GDPR compliance by raising knowledge of and demand for privacy rights.[215]

3.3.3 Economic Factors: Ireland's economy is home to many global companies, especially in the technology industry, that can afford to invest in sophisticated data protection plans.[216] These businesses may guarantee strong GDPR compliance by utilising their financial strength. Small and medium-sized businesses (SMEs) in Ireland, however, sometimes have financial difficulties in fulfilling GDPR obligations, creating an unequal playing field regarding data protection skills.[217] The impact that economic differences have on data protection compliance among different-sized organisations is covered in Sheila FitzPatrick's book. She pointed out that while larger businesses can afford the infrastructure required for

[212] Karen McCullagh, *Data Protection Law: Approaches to Privacy Governance in the EU and US* (Cambridge University Press 2020).
[213] Karen McCullagh, *Data Protection Law: Approaches to Privacy Governance in the EU and US* (Cambridge University Press 2020).
[214] *Ibid.*
[215] Nessrine Omrani, Francesco Schiavone, and Christine Amir, 'Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe' (2024) *Information Technology & People* https://doi.org/10.1108/ITP-05-2023-0467 accessed 7 August 2024
[216] Greenleaf, G. 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2018) 157 *Privacy Laws & Business International Report* 14-18.
[217] *Ibid.*

compliance, SMEs find it difficult to make ends meet, which can impede the adoption of consistent data protection laws throughout the economy.[218]

3.4 Discussion on the Impact of These Factors on the Right to Privacy

This section deals with a discussion on whether the factors discussed in 3.3 has a positive or negative impact on the right to privacy.

Cultural values play a pivotal role in shaping the implementation of data protection laws. In countries like Ireland which was used as a case study, where individual rights and privacy are deeply embedded in the cultural fabric, the enforcement of GDPR provisions is more stringent. This cultural predisposition towards valuing privacy facilitates a higher level of compliance among organizations and individuals. For instance, McCullagh's research highlights that nations prioritizing individual rights tend to enforce strict data privacy laws more effectively.[219] This cultural alignment with the principles of GDPR ensures that the right to privacy is not only a legal obligation but also a societal norm, thereby enhancing overall compliance and protection. Digital literacy and public attitudes towards technology also significantly affect the enforcement of GDPR. High levels of digital participation and a tech-savvy populace, as seen in Ireland, lead to greater awareness and assertion of privacy rights. Donovan's study underscores the relationship between digital literacy and GDPR compliance, suggesting that informed and technologically adept citizens are more likely to demand accountability from organizations regarding their data practices.[220] This awareness and proactive stance among the public ensure that privacy rights are not merely theoretical but actively exercised and protected in practice.

Economic factors introduce another layer of complexity in enforcing the right to privacy. The disparity between large multinational corporations and small to medium-sized enterprises (SMEs) in terms of resources available for GDPR compliance creates an uneven playing field. While global companies can afford sophisticated data protection measures, SMEs often struggle with the financial burden of compliance. Fitzpatrick's analysis reveals that this

[218] Sheila FitzPatrick (ed), *Global Data Privacy: Building Trust in the Digital Economy* (Oxford University Press 2021) 112-130
[219] Karen McCullagh, *Data Protection Law: Approaches to Privacy Governance in the EU and US* (Cambridge University Press 2020)
[220] Nessrine Omrani, Francesco Schiavone, and Christine Amir, 'Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe' (2024) *Information Technology & People* https://doi.org/10.1108/ITP-05-2023-0467 accessed 7 August 2024

economic divide impacts the consistency of data protection across different business sizes.[221] Despite these challenges, the GDPR's uniform legal framework aims to provide a baseline of protection, although practical enforcement may vary depending on the economic capabilities of the entities involved. In the area of technological advancement, Nessrine's study highlights how GDPR has spurred innovation in data protection technologies, ensuring that businesses can better safeguard personal information.[222] This technological push not only enhances the right to privacy but also builds trust in digital services, fostering a safer digital environment. In conclusion, the cultural attitude of and EU jurisdiction, seem to positively impact on the practical implementation of right to privacy. However, the unstable discrepancy between small- and large-scale businesses could pose a minor hinderance but overall, it can be concluded that these factors does not in its totality impede on the true adherence to right to privacy.

3.5 CONCLUSION

Chapter 3 analyses key GDPR provisions—access, rectification, data portability, and protection from automated decision-making—highlighting their role in enhancing transparency and individual control over personal data. Landmark cases like Schrems and Google Spain SL illustrate the significance of these rights. The chapter also details GDPR enforcement mechanisms under Articles 51, 57, 58, and 70, showcasing the effectiveness of supervisory authorities and the EDPB through actions against major firms like Google and Meta. Additionally, it examines Ireland's GDPR implementation, noting the positive impact of its privacy culture and digital literacy, alongside challenges faced by smaller businesses.

[221] Sheila FitzPatrick (ed), *Global Data Privacy: Building Trust in the Digital Economy* (Oxford University Press 2021)
[222] Nessrine OMRANI, Francesco Schiavone, and Christine Amir, 'Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe' (2024) Information Technology & People.

CHAPTER 4

COMPARATIVE ANALYSIS OF LEGAL PROVISIONS, ENFORCEMENT MECHANISMS AND IMPLEMENTATION CHALLENGES

INTRODUCTION

This chapter focuses on a doctrinal comparison of the rights of data subjects provided for in the GDPR and NDPA in addition to a comparison of the enforcement mechanisms provided in these legislations to uphold the right to privacy. The rights to be compared are right of access, right to rectification, right to data portability and right related to automated decision making. This chapter will also proffer a comparative analysis of the factors which affect the proper administration of the legislations viz cultural, economic and social factors. The last part of this chapter will compare how these factors affect privacy protection in both jurisdictions (Nigeria and Ireland representing the EU). This chapter will draw insight from chapter 2 and 3 of this work to effectively make these comparisons.

4.1 Comparative analysis of Data Subject Rights

The data subject rights provided in the GDPR and NDPA seem to be quite similar. For example, section 34(a) of the NDPA provides for right to access and same right was provided for in Article 15 of the GDPR as detailed ineptly in chapter 2 and 3. This sub-heading deals with a comparison of these rights provided.

4.1.1 A comparative Analysis of the Right to Access under the NDPA and GDPR

The GDPR contains two introductory articles in 13 and 14 which broadly described the background to the rights of a data subject and sets out requirements for transparency, ensuring that individuals are informed about their personal data and its processing.[223] This background includes situations where data is collected directly from the data subject from instance when a person fills an electronic form online.[224] The second category is when data is collected by a third-party example if an organization receives data from credit bureaus or

[223] General Data Protection Regulation [2016] OJ L119/40. General Data Protection Regulation [2016] OJ L119/41.
[224] *Ibid.*

other external sources i.e. how organizations sometimes rely on data collected by other entities to enhance their own information resources and decision-making processes. [225] It contains privacy information such as Organization's name and contact details, purpose of processing, legal basis for processing, categories of personal data collected, recipients or categories of recipients of the data, retention periods for the data, rights available to individuals regarding the processing, right to withdraw consent (if applicable), right to lodge a complaint with a supervisory authority and source of the personal data (if not obtained directly from the individual).[226]

Following the foundation laid in article 13 and 14, the right of access became inherent in article 15 of the GDPR. This article enables people to find out from data controllers whether their personal data is being processed or not. People have the right to access their personal data and obtain thorough information about the processing activities if processing is in fact occurring,[227] Information on the processing's goals,[228] the categories of personal data processed,[229] the recipients or groups of recipients to whom the data has been or will be revealed,[230] and the anticipated length of time the data will be kept are all included in this.[231] Furthermore, people are entitled to knowledge about automated decision-making, including profiling, and to relevant information regarding the reasoning behind it, the importance of the processing, and the expected outcomes.[232] On the other hand, the NDPA like the GDPR has a broad section which offers an introductory description of privacy information. But on a deep examination of the section reveals that both privacy information on the right of access, and a few other rights were all merged into one section. What does this mean? Section 34 of the NDPA outlines the rights of data subjects and the obligations of data controllers regarding the processing of personal data. It emphasizes the importance of transparency and accountability in data handling practices Just like the GDPR in article 13 and 14. We can therefore conclude that in this segment, the NPDA and GDPR offer similar provisions.

Next, in section 34 of the NDPA, Data subjects have the right to ask data controllers whether their personal data is being processed.[233] They further have the right to full information about

[225] *Ibid.*
[226] *Ibid.*
[227] General Data Protection Regulation [2016] OJ L119/43.
[228] General Data Protection Regulation [2016] OJ L119/43.
[229] General Data Protection Regulation [2016] OJ L119/43.
[230] General Data Protection Regulation [2016] OJ L119/43.
[231] General Data Protection Regulation [2016] OJ L119/43.
[232] General Data Protection Regulation [2016] OJ L119/43.
[233] Nigerian Data Protection Act 2023, s 34(a).

the purposes, categories of data, recipients, durations of storage, and whether automated decision-making processes are being used, if processing is occurring. This ensures that individuals are fully informed about the use of their data and who can access it, but this is subject to the discretion of the data controller who the responsibility rests on to disclose. On the other hand, the GPDR, having similar provision on the duties imposed on the data controller to provide the data subject with this information, there is still a separate provision which guides the data subject on the way they can exercise this right. This was provided for separately in article 12 of the regulation.[234] What this implies is that the GDPR has sought to reduce excessive power on the data controller and rather granted power to the data subjects on how their rights can be exercised. This is not the case in the NDPA as there is no provision which describes how data subjects can exercise their rights rather that guide was placed solely in the hand of the NDPC.[235]

Furthermore, in article 15(3) it was stated that a data subject is entitled to a copy of personal data but then if he would require further copies, the data controller would have to charge him a reasonable administrative fee.[236] This part of the article says nothing about undue hardship that could possibly be suffered by the data controller if the costs for providing copies is high. On the other hand, the NDPA in article 34(b) has a similar provision in relation to granting the data subject right to obtain copies of his data, however, he would bear the cost of providing the copies will cause undue hardship to the data controller.[237] This part of the section says nothing about situations where the data subject requests for additional copies. If this information is analysed from one aspect, we could say that the NDPA could be more versatile in this context because, a regulation which has proffered solution to a potential problem for the data controller in respect of fees payable could be considered more comprehensive than one which provides for costs for additional copies only, paying more attention to the financial needs of the data controller than the data subjects.

4.1.2 **A comparative Analysis of the Right to Rectification**

The right to rectification is provided for in article 15 of the GDPR but then a separate article was afforded to this right for a better and broader provision for the data subjects. This is provided for in article 16 of the GDPR. According to this article, people have the right to

[234] General Data Protection Regulation [2016] OJ L119/40.
[235] Nigerian Data Protection Act 2023, s 6.
[236] General Data Protection Regulation [2016] OJ L119/43.
[237] Nigerian Data Protection Act 2023, s 34(b).

have erroneous personal data corrected.[238] This implies that individuals can ask the data controller to quickly update any inaccurate information that is kept about them. The requirement that the rectification be made right away emphasises how crucial it is to act quickly to guarantee that the data subject's information is accurate as soon as feasible. Furthermore, the article goes further to add that individuals have the right to have their incomplete personal data completed in addition to having errors corrected.[239] This guarantees that all pertinent data is completely recorded and appropriately depicts the circumstances of the data subject. The person can contribute extra information to the data to make it complete and correct. This could entail providing more context or specific specifics. In addition to article 16, the GDPR in article 15(1)(e), stated that the data subject has the right to be informed by the data controller that he could rectify his data. In addition, Like the right of access, the GDPR has set forth in section 12 on how all the rights contained in article 15-22 can be exercised. The exercise of this right was described in chapter 3 of this work. Despite this, obligation is still placed on the data controller to inform the data subjects of any rectification that has been done on his data. This creates a balanced form of shared power between the data controller and the data subjects, and this makes for the interest of the data subjects to properly enjoy their data right to rectification among others.

On the other hand, the NPDA in section 34(1)(a)(v) generally provided that the data subject should be informed of their right to rectification, erasure, and restriction of processing. This section compressed three rights in one line with not further explanation or detailed information. There is no other section that provided for a broader explanation on what rectification could mean like the GDPR explained in article 16. Despite this disparity, it could stand that the draftsmen of the NDPR used the word in its literal sense ‘rectify’ which means ‘amend’ according to the oxford dictionary.[240] Unlike the GDPR, the NDPA falls short of a provision which describes how the right to rectification can be exercised. It only provided in section 24(e), that the data controller is obligated to inform the data subject of any rectification when they deem it appropriate. This places too much power on the data controller thereby dimming the power of the data subject to exercise their rights. Also, unlike the GDPR, section 34(1)(a)(v) has no further provision on completion of incomplete data, and this creates a lacuna in the law.

[238] General Data Protection Regulation [2016] OJ L119/43.
[239] General Data Protection Regulation [2016] OJ L119/43.
[240] Oxford Learner's Dictionary (Oxford University Press 2020).

4.1.3 A comparative Analysis of the Right related to automated decision making

Both the NDPA and GDPR seem to offer similar provision for right not to be subject to automated decision making. This right is contained in the first part of Section 37 of the NDPA and in article 22 of the GDPR. In section 37 of the NDPA, it is stated that no decision pertaining to a data subject shall be made exclusively based on automated processing of personal data, including profiling, if doing so has a substantial impact on their legal status or other matters.[241] This clause acknowledges the dangers and negative effects like unfair discrimination or exclusion that automated decision-making procedures may cause.[242] However, the Act also acknowledges that there are situations where automated decision-making may be necessary or beneficial in subsection 2, thereby proffering their exceptions. These exceptions include cases where the decision is necessary for entering into or performing a contract between the data subject and a data controller, cases where the decision is authorized by a written law that safeguards the fundamental rights and freedoms of the data subject, and cases where the decision is authorized by the consent of the data subject.[243] These exceptions pose a balanced approach that allows for the use of automated decision-making in some circumstances while still protecting the rights of data subjects. Finally, Subsection 3 of Section 37 mandates that data controllers implement suitable measures to safeguard the data subject's fundamental rights, freedoms, and interests.[244] These measures include the right to obtain human intervention on the part of the data controller, the right to express the data subject's point of view, and the right to contest the decision.[245] This provision ensures that data subjects are not left powerless in the face of automated decision-making processes and that they have avenues for recourse if they believe their rights have been violated. However, the downside about this right is that data subjects are not informed about how they can exercise this right which is same issue that has been identified in the two rights examined above.

On the other hand, Article 22 of the GDPR deals with automated decision making. Article 22, paragraph one, states that a person who provides information has the right to be free from decisions that are made exclusively based on automated processing, including profiling, if those decisions have a substantial impact on the data subject or result in legal ramifications

[241] Nigerian Data Protection Act 2023, s37.
[242] Nigerian Data Protection Act 2023, s 37(1).
[243] Nigerian Data Protection Act 2023, s 37(2).
[244] Nigerian Data Protection Act 2023, s 27(3).
[245] Nigerian Data Protection Act 2023, s 37(3).

for them[246]. Some exceptions to this privilege are stated in the second paragraph listing circumstances exempt the decision from its application. These include contracts that the data subject and the data controller must enter or perform, decisions authorised by Union or Member State law to which the controller is subject and that specifies appropriate safeguards for the data subject's rights, freedoms, and legitimate interests, and decisions based on the data subject's explicit consent.[247] The provision further mandates that an organisation, referred to as the "data controller," must put appropriate safeguards in place to protect an individual's rights, freedoms, and legitimate interests when a decision is made solely based on automated processing of personal data and is either required by contract or based on the individual's explicit consent.[248] This basically implies that the data controller is responsible for making sure the automated decision-making process respects the rights of the individual. Among these protections are the rights of the person to request human intervention from the data controller, voice their objection, and challenge the decision.[249] Put another way, you have the right to have a human from the organisation review any decision made about you by a machine or algorithm, to express your own opinion, and to contest the conclusion if you don't agree with it.

In addition, special categories of personal data, or data that is deemed more sensitive and so needs more protection, are covered under the second clause. Information about a person's race, ethnic origin, political ideas, religious beliefs, trade union membership, genetic information, biometric information, health information, and information on their sexual orientation or sex life are a few examples of specific categories of personal data.[250] This provision states that unless an individual has explicitly consented to the use of their data or processing is required for reasons of substantial public interest as defined by Union or Member State law, decisions based on automated processing should not be based on these special categories of personal data.[251]

By way of comparison, Section 37 of the NDPA and Article 22 of the GDPR aim to safeguard individuals from judgements that are made only by automated processing, such as profiling. They both offer exceptions when such automated decision-making is required by law,

[246] General Data Protection Regulation [2016] OJ L119/46.
[247] General Data Protection Regulation [2016] OJ L119/46.
[248] General Data Protection Regulation [2016] OJ L119/46.
[249] General Data Protection Regulation [2016] OJ L119/46.
[250] General Data Protection Regulation [2016] OJ L119/46. General Data Protection Regulation [2016] OJ L119/38.
[251] *Ibid.*

required for the fulfilment of a contract, or based on the express consent of the individual. In addition, both demand that data controllers put appropriate safeguards in place to protect the person's rights, freedoms, and legitimate interests. But the GDPR goes a step further and states that unless specific requirements are satisfied, decisions cannot be made using special categories of personal data while also stipulating how this right should be exercise in article 12 of the regulation. This emphasises how important it is for sensitive personal data to be protected under GDPR. In essence, the NDPA falls short of the provision of including special category data as exceptions to the right to automated decision making.

4.1.4 A comparative Analysis of the Right to Data Portability

The right to data portability allows people take ownership of their personal data. It offers them the right to quickly and in an organised, widely used, and machine-readable way get their personal data from a data controller. Nevertheless, this right also enables people to transfer their personal information to another data controller without facing any obstacles.[252] Simply put, you can take your data (contacts and emails, for instance) with you if you're changing email providers. Furthermore, data can be sent straight from one data controller to another if it is technically feasible.[253] This implies that the corporations must carry out the bulk of the work. They handle the transfer's specifics when you request that your data be transferred. The Commission, the body in charge of these rules, can determine the precise terms and conditions that people can use to exercise their right to data portability. They are also able to ascertain the responsibilities of the data controllers and processors, including financial and schedule-related issues.[254] On the other hand, The GDPR, like the NDPA, in article 20 enables people to access and reuse their personal data across other services.[255] This implies that people have the right to obtain their personal data in a machine-readable, structured, and widely used format that they have supplied to a data controller.[256] If the processing is done automatically and is based on permission or a contract, they also have the freedom to transfer this data to another data controller without any restrictions.[257] Additionally, when technically possible, people have the right to have their personal data transferred directly from one data controller to another.[258] This right does not, however,

[252] Nigerian Data Protection Act 2023, s 38.
[253] Nigerian Data Protection Act 2023, s 38.
[254] Nigerian Data Protection Act 2023, s 38.
[255] General Data Protection Regulation [2016] OJ L119/45.
[256] General Data Protection Regulation [2016] OJ L119/45.
[257] General Data Protection Regulation [2016] OJ L119/45.
[258] General Data Protection Regulation [2016] OJ L119/45.

extend to processing that is required to carry out an activity that serves the public interest or to exercise official power that has been granted to the controller.[259] Furthermore, exercising this right shouldn't have a negative impact on other people's freedoms and rights.[260]

When compared to Section 38 of the Nigeria Data Protection Act (NDPA), both clauses seem to corelate in the right to data portability, which grants people the ability to transfer their personal data to another data controller and receive it in a structured, widely used, and machine-readable manner. The NDPA, however, takes a step further by giving the Commission the authority to create regulations outlining the right to the portability of personal data as well as to specify the situations and requirements under which the data subject may use this right. This covers the responsibilities it would place on a data controller or processor, such as those related to expenses and timeliness. Though there is no assurance that these regulations will be favourable the obligation placed on the NDPC to stipulate them demonstrates that the NDPA takes a more thorough and controlled approach than the GDPR in this area. It is also important to mention in the part that the NDPA has no designated section for how the data subject can exercise this right but rather so much attention is place on the NDPA to determine how this right is run rather than giving due consideration to the person directly affected by this right.

4.2 Comparative assessment of enforcement mechanisms within NPDA and GDPR

In this part, a comparison of enforcement mechanisms of both laws will be rendered. Recla that in 2.2 and 3.2, an in-dept analysis was done on the enforcement mechanism of both laws and now, these mechanisms will be compared below. The Nigeria Data Protection Act (NDPA) mainly describes the enforcement mechanisms in the sections 5 and 6 of the Act, which is part of the focus of this work. Article 5 delineates the obligations of the Nigeria Data Protection Commission (NDPC), which is the entity responsible for implementing the Nigeria Data Protection Act (NDPA). They were afforded several responsibilities which includes regulating Measures to improve personal data protection, i.e. they establish the guidelines for how businesses must safeguard personal information.[261] Also, they are responsible for facilitating the advancement of personal data protection technologies by ensuring that they comply with global best practices and relevant international law,[262] accreditation and

[259] General Data Protection Regulation [2016] OJ L119/45.
[260] General Data Protection Regulation [2016] OJ L119/45.
[261] Nigerian Data Protection Act 2023, s 5(a).
[262] Nigerian Data Protection Act 2023, s 5(b).

Licencing,[263] registration of Data Controllers and Processors,[264] raising awareness,[265] raise public knowledge and comprehension of the risks to breach of personal data,[266] receiving complaints[267], purchasing assets.[268] And lastly a discretion to undertake additional acts.[269]

To guarantee that the NDPA is implemented effectively, the NDPC is endowed with several authorities in section 6 of the Act. Its main responsibility is to supervise the application of the Act's provisions, making sure that the guidelines are followed accurately and efficiently in real-world situations.[270] The NDPC is also able to determine the fees that data controllers and data processors must pay. These fees are a type of regulatory expense associated with managing personal data, usually commensurate with the volume of data processing operations carried out by these businesses.[271] The NDPC is authorised to issue rules, regulations, guidelines, and directives to give clarification and guidance on the provisions of the Act. This aids entities in understanding the Act's requirements and how to meet them.[272] Monitoring compliance is another responsibility of the NDPC. It can ascertain how often and how data controllers and processors of significant importance file compliance returns.[273] In essence, these returns are reports that show how these organisations are complying with the Act. The NDPC may request information from anyone and examine any records pertaining to Act-related activities to investigate possible violations of the Act. Data controllers and data processors may be the subject of investigations by the NDPC if a violation is detected.[274] Lastly, fines for any breach of the Act or its ancillary laws may be imposed by the NDPC.[275] This acts as a deterrent, motivating organisations to respect the data privacy laws outlined in the Act and discouraging non-compliance. We can conclude from the discussion of these section that the NDPA rests its enforcement power solely on the NDPC. While we can say that this is a good innovation because the powers, functions and duties mentioned tend to encapsulate contents that ensure the Act is being compiled with thereby, protecting the

[263] Nigerian Data Protection Act 2023, s 5(c).
[264] Nigerian Data Protection Act 2023, s 5(d).
[265] Nigerian Data Protection Act 2023, s 5(e).
[266] Nigerian Data Protection Act 2023, s 5(f).
[267] Nigerian Data Protection Act 2023, s 5(g).
[268] Nigerian Data Protection Act 2023, s 5(h).
[269] Nigerian Data Protection Act 2023, s 5(i).
[270] Nigerian Data Protection Act 2023, s 6(a).
[271] Nigerian Data Protection Act 2023, s 6(b).
[272] Nigerian Data Protection Act 2023, s 6(c).
[273] Nigerian Data Protection Act 2023, s 6(d).
[274] Nigerian Data Protection Act 2023, s 6(d).
[275] Nigerian Data Protection Act 2023, s 6(d).

stipulated data subject rights, it can be argued that usurping power solely into one body could potentially lead to an abuse of power.

On the other hand, it appears that the General Data Protection Regulation (GDPR) enforces its provision by using a decentralised approach. Several GDPR clauses have different enforcement mechanisms such as article 55-59, and articles 77- 84. But for the purpose of limitation, attention will only be drawn to the enforcement mechanisms contained in article 51, 57,58 and 70 of the regulation as discussed in 3.3 above. The General Data Protection Regulation (GDPR) of the European Union employs a decentralized enforcement mechanism through the establishment of independent supervisory authorities in each member state. Articles 51, 57, and 58 of the GDPR outline the creation, tasks, and powers of these authorities. Each member state must provide for one or more supervisory authorities responsible for monitoring GDPR application, ensuring the protection of data subject rights, and facilitating the free flow of personal data within the Union. The supervisory authorities are tasked with promoting public awareness, advising national institutions, handling complaints, and cooperating with other authorities to ensure consistent application of the GDPR. Article 58 provides these authorities with a comprehensive range of investigative, corrective, and advisory powers, enabling them to conduct audits, issue fines, and provide guidance on data protection matters. The European Data Protection Board (EDPB), established under Article 70, further ensures uniform application of the GDPR across the EU by issuing guidelines, recommendations, and opinions. Following the above illustration, the GDPR has provided several bodies for ensuring that data subject rights are adhered to. In addition, the introduction of checks and balances amongst the system suggest a balanced approach. For a better understanding, a comparison of the enforcement mechanism of both laws is tabularised below.

4.2.1 Hierarchy of enforcement bodies

	GDPR (Decentralised)	**NDPA (Centralised)**
Top Level	European Data Protection Board (EDPB)	Nigeria Data Protection Commission (NDPC)
Middle Level	National Data Protection Authorities (DPAs) in each EU member state	Not applicable

Ground Level	Data controllers and data processors in each EU member state	Data controllers and data processors across Nigeria

The European Data Protection Board (EDPB), which publishes rules and recommendations, is the primary enforcement body for the GDPR. The national Data Protection Authorities (DPAs) in each EU member state are the next level, and they are responsible for enforcing the GDPR within their respective jurisdictions. Finally, each EU member state's data controllers and processors bear primary responsibility for adhering to the GDPR.

On the other hand, the NDPA uses a centralised approach of operation. The Nigeria Data Protection Commission is the first and last stop for enforcement (NDPC). The NDPC registers data controllers and processors of significant importance, controls the deployment of measures to improve personal data protection, and supervises the execution of the Act's provisions. The NDPA must be complied with by data controllers and processors throughout Nigeria. This hierarchy does not have a mid-level because all data controllers and processors in Nigeria are directly under the direct supervision of the NDPC.

Lastly, the enforcement mechanism of the GDPR is exemplified in the case of The French Data Protection Authority where Meta Platforms Ireland Limited, formerly Google, was fined €1.2 billion by the French Data Protection Authority (DPA), also referred to as the CNIL, for illegally transferring personal data to the US.[276] The CNIL concluded that Google had not provided its consumers with easy access to its consumer data processing statements. Furthermore, Google was found guilty of using user data for targeted advertising efforts without first obtaining consent. The higher court in France dismissed Google's appeal and affirmed the fine.[277] Regretfully, there are no reported case laws on the judicial interpretation of the enforcement of the NDPA. This might be the result of the act having only been implemented in 2023 and the lack of documented cases pertaining to the act. However, since the NDPA empowers the Nigerian Data Protection Commission (NDPC) to enforce compliance with data protection laws and impose penalties for non-compliance, it simply means that most cases could be directed to NDPC.

[276] Commission Nationale de l'Informatique et des Libertés (CNIL), 'Sanction Pronounced Against Futura Internationale' (27 December 2018) Decision No SAN-2018-011.
[277] *Ibid.*

4.3 Comparative investigation of factors affecting the enforcement of the GDPR and NDPA

This investigation deals with a comparison of the factors discussed in chapter 2 and 3 above and how they have affected the implementation of privacy protection mechanism. In this case, this work will weigh side by side the pros and cons of each jurisdictional factor that has influenced data privacy. This comparative analysis will be split into socio-economic and socio-cultural factors.

4.3.1 Socio-Economic Factors

The socioeconomic environment in the EU is comparatively homogeneous, and there is a strong public demand for data privacy and understanding of its rights.[278] This consistency makes it easier for member states to apply the GDPR because privacy and consumer protection are valued and understood similarly.[279] There is a strong consumer protection rules in the EU that support data privacy laws. The protection of consumer rights is guaranteed by these provisions, which raises the GDPR's overall efficacy.[280] A vibrant civil society within the European Union (EU), comprising diverse non-governmental organisations (NGOs) and advocacy groups, advocates for data privacy, and ensures corporate responsibility.[281] For instance, the support provided by Max Schrems and his group NOYB (None of Your Business) has resulted in important decisions regarding data privacy, such as the Court of Justice of the European Union (CJEU) invalidating the EU-US Privacy Shield in the Schrems II case.[282] The famous case *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[283] highlights the real-world implications of the GDPR. The CJEU determined that search engines are data controllers in this instance and are obligated to abide by data protection laws.[284] This case highlighted the strict implementation of the GDPR and its effects on international data practices, setting a precedent for online data privacy.

[278] European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities* (2020)
[279] *Ibid.*
[280] Ibid.
[281] *Ibid.*
[282] Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Schrems II) [2020] ECLI:EU:C: 2020:559.
[283] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317.
[284] *Ibid.*

On the other hand, the implementation of NDPA faces significant challenges due to limited financial and human resources.[285] It is commendable that the NDPA established the NDPC to replace the NDPB of the NDPR, however, there is still work to be done. Nigerians' disparate degrees of internet literacy provide yet another significant obstacle.[286] Rural communities frequently fall well behind of urban ones in terms of digital literacy. It is challenging to guarantee that data privacy laws are widely understood and followed because of this disparity.[287] Education and public awareness regarding data protection rights is vital. Many people are not aware of their NDPA rights, which makes it difficult for them to use such rights effectively.[288] Nigeria's heterogeneous socioeconomic landscape poses difficulties for data protection.[289] Regional differences in wealth have an impact on how well the NDPA is implemented. Compared to impoverished, rural places, wealthier regions with superior infrastructure can comply with data protection regulations more readily.[290] Another major obstacle to the successful implementation of the NDPA is the inadequate digital infrastructure in many parts of Nigeria.[291] The uneven distribution of internet adoption and technology access affects the capacity to apply data protection rules consistently.[292] Different cultural perspectives on privacy have an impact on how the NDPA is implemented as well. Individual privacy may not be as highly valued, which may influence the adoption and application of data protection laws.

4.3.2 **Socio- Cultural Factors**

Ireland’s cultural environment, deeply rooted in its political, social, and historical contexts, significantly influences its data protection laws. The individualistic focus of EU data privacy regulations, such as GDPR, often clashes with Ireland’s cultural emphasis on community and collective well-being. This dichotomy manifests in a more collective approach to data privacy, where the community’s needs and values are balanced against individual rights. Ireland’s long history of local government and public participation encourages vigilance about data usage and the enforcement of necessary measures.[293] However, this communal focus

[285] United Nations Conference on Trade and Development, *Digital Economy Report 2021* (United Nations 2021)
[286] National Information Technology Development Agency, *National Digital Literacy Framework* (2019)
[287] *Ibid*.
[288] *Ibid.*
[289] World Bank, *Nigeria Digital Economy Diagnostic Report* (World Bank Group 2020)
[290] *Ibid.*
[291] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2020* (2020)
[292] African Union Commission, *The State of Data Privacy Laws in Africa* (2019)
[293] Greenleaf, G. ‘Global Data Privacy Laws 2019: 132 National Laws & Many Bills’ (2018) 157 *Privacy Laws & Business International Report* 14-18.

might also lead to challenges in prioritizing individual data subject rights, as local cultural norms may take precedence[294]. In Nigeria, cultural perceptions of privacy often significantly differ from Western conceptions. Privacy is frequently viewed within the context of community and family rather than as an individual right.[295] This communal perspective could complicate the enforcement of data protection laws designed to safeguard individual privacy rights.[296] The communal nature of Nigerian societies means that data sharing within families and communities is common, potentially leading to unintentional breaches of privacy laws.[297]

Both Ireland and Nigeria have cultural factors that influence the implementation and enforcement of data protection laws. In Ireland, the emphasis on community and collective well-being can sometimes conflict with the individualistic focus of EU data privacy regulations. On the other hand, in Nigeria, the communal nature of societies and the common practice of data sharing within families and communities can complicate the enforcement of data protection laws designed to safeguard individual privacy rights.

4.4 Comparison on how these factors affect privacy protection.

A comparative analysis of the enforcement mechanisms of GDPR and NDPA reveals distinct impacts on the right to privacy due to differing cultural, social, and economic contexts. The GDPR benefits from a culturally ingrained respect for individual privacy rights within the EU, particularly in countries like Ireland, leading to stringent enforcement and higher compliance. High digital literacy rates and public awareness further bolster the effectiveness of GDPR enforcement, ensuring that privacy rights are actively exercised and protected. Economic disparities do exist, but the GDPR's comprehensive legal framework and the technological advancements it spurs help mitigate these challenges, providing a baseline of protection that enhances the right to privacy across different business sizes.

In contrast, the NDPA faces more significant hurdles due to Nigeria's cultural, social, and economic landscape. The communal view of privacy complicates individual data protection efforts, necessitating culturally tailored awareness initiatives. Low levels of digital literacy impede public understanding and assertion of privacy rights, highlighting the need for extensive educational campaigns. Economically, the high cost of compliance presents a

[294] *Ibid.*
[295] Achuonye KA, 'Digital Literacy and Primary Educational System in Nigeria' (2012) 3 Journal of Educational and Social Research 1.
[296] S A Oluwadare and F A Adebesin, 'Data Protection in Nigeria: The Current State and Future Directions' (2022) 12 Journal of Nigerian Law and Technology 45-67.
[297] *Ibid.*

substantial barrier for SMEs, requiring government intervention in the form of financial incentives and training programs to improve adherence to the NDPA. These factors collectively result in a less effective enforcement mechanism compared to the GDPR, negatively impacting the right to privacy in Nigeria. In conclusion, while both GDPR and NDPA aim to protect data privacy, the GDPR's enforcement is bolstered by favourable cultural, social, and economic conditions in the EU, leading to a more positive impact on the right to privacy. Conversely, the NDPA's enforcement is hindered by Nigeria's unique challenges, necessitating additional measures to enhance the protection of privacy rights effectively.

4.5 CONCLUSION

This chapter dealt with an in-depth comparison of the selected data subject rights discussed in chapters 2 and 3 above. The comparison reveals that while both laws seek to protect privacy rights, the GDPR seem to be more elaborate compared to the NDPA in its provisions. Further analysis reveals that unlike the GDPR, the NDPA falls short of a provision for how these rights can be enforced. Furthermore, comparison revealed that the GDPR seem to have a decentralised enforcement approach while the NDPA has a centralised one which could lead to aa abuse of power thereby deviating for the sole them of this work which is upholding right to privacy. Finally, this work compared some factors affecting implementation and the comparison reveals that the factors in Nigeria impede on enforcement compared to the GDPR.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

INTRODUCTION

This chapter focuses on a collation of the key findings that was discovered during this research. The key findings will be drawn from chapter 2 and 3 in the analysis of both frameworks specifically on their provisions that this works relates. In addition, insight will be drawn from chapter 4 where the comparative analysis was done. Lastly, this chapter conclude by proffering recommendation drawn from comparative analysis, recommendation for policy makers and lastly make suggestion for future research and suggestions to enhance enforcement mechanisms in both jurisdictions.

5.1 **Summary of key findings**

a. Right to Access

This right ensures accountability and transparency. Articles 13 and 14 of the GDPR provide the foundation by describing the information that must be given to data subjects, including the recipients, categories of personal data, and the reasons for data processing. Article 15 also gives people the ability to find out if their data is being processed and to get detailed information about what is being processed. On the other hand, the NDPA combines these rights under Section 34, which describes the rights and obligations of data subjects as well as data controllers. Although this consolidation may make things easier to grasp, it may also make certain rights that are more precisely defined in the GDPR less obvious. Although transparency is emphasised in both frameworks, the GDPR's precise division of rights appears to provide clearer guidance. Also, it is revealed that the NDPA does not have any provision which proffers a guide on how the rights listed in section 34 can be exercised. On the other hand, the GDPR seem to have addressed this issue in Article 12(3) and (4).

b. **Right to Rectification**

Article 16 of the GDPR grants people the right to rectification, which enables them to quickly complete missing information and amend wrong data. This right aids in preserving the integrity and correctness of data. Furthermore, this right is further strengthened by Article

15(1)(e), which guarantees that data subjects are informed of their right to have their data corrected. However, the right to rectification is mentioned in Section 34(1)(a)(v) of the NDPA without any further clarification. It appears that the phrase "rectify" is being applied broadly, in its literal sense which may not have the same level of detail as the GDPR. As a result, even though both frameworks emphasise the value of accurate data, the GDPR appears to provide a more thorough and explicit method for the right to rectification.

Furthermore, it is discovered that the data protection officer in the NPDA seem to possess more power in the exercise on this right than the actual owner of the right – Data subjects. Whereas in the GDPR this power is shared between the data controller and the data subjects where the data subject has the right to request for a rectification as provided for in article 12 of the GDPR.

c. **Right related to Automated Decision-Making**

Article 22 of the GDPR restricts decisions based solely on automated processing, including profiling, if they significantly affect individuals. It provides exceptions and requires safeguards, such as the right to human intervention and the ability to contest decisions. This article also emphasizes the protection of special categories of personal data. Similarly, Section 37 of the NDPA restricts automated decision-making and includes exceptions. It mandates safeguards to protect data subjects' rights, including human intervention and the right to contest decisions.

d. **Right to Data Portability**

The right to data portability, outlined in Article 20 of the GDPR, allows individuals to receive their data in a structured, commonly used, and machine-readable format and to transfer it to another controller. This right applies when processing is based on consent or a contract and is carried out by automated means. Section 38 of the NDPA provides a similar right but goes further by allowing the Commission to create regulations specifying the conditions and responsibilities for data portability, including costs and timelines.

e. **Enforcement Mechanisms**

The GDPR employs a decentralized enforcement approach with supervisory authority(s) in each EU member state, coordinated by the European Data Protection Board (EDPB) and acts as checks amongst one another. Articles 51, 57, 58 and 70 outline these roles and powers of these authorities, including the ability to impose fines and conduct investigations. This is

exemplified in the cases where fines were imposed on google and HnM for alleged breach of data rights. In contrast, the NDPA uses a centralized enforcement mechanism through the Nigeria Data Protection Commission (NDPC). Sections 5 and 6 describe the NDPC's functions and powers, including registration, licensing, compliance monitoring, and the ability to impose fines. The GDPR's decentralized approach allows for localized enforcement and coordination across the EU, while the NDPA's centralized approach consolidates power within a single authority which could pose a challenge for proper administration thereby giving room for abuse of power.

5.2 Recommendations drawn from comparative analysis

Based on a comparative analysis of data subject rights under the GDPR and the NDPA, several recommendations can be made.

Firstly, the NDPA should adopt the GDPR's broader provisions regarding the rights to access, rectification, and automated decision-making. The GDPR offers more comprehensive definitions and details concerning these rights, which could enhance the NDPA's framework.

Additionally, the NDPA would benefit from mirroring the GDPR's approach to the exercise of data subject rights by incorporating a dedicated section like Article 12 of the GDPR. This section outlines how data subjects can exercise their rights, providing clear guidance and procedures. Conversely, the GDPR could take a cue from the NDPA regarding the right to data portability. The NDPA provides specific provisions on how costs associated with exercising this right are handled, which could serve as a model for the GDPR.

Furthermore, the GDPR should consider aligning with the NDPA's stipulations on cost-bearing responsibilities. The GDPR leaves the determination of costs to the discretion of the Data Protection Officer (DPO), whereas the NDPA explicitly states that the data controller is responsible for covering these costs. Adopting a similar approach in the GDPR could streamline the process and ensure clarity regarding financial responsibilities for data subject rights**,** thereby reducing financial hardship on the data subject.

5.3 Recommendations for Policymakers

To enhance data protection and align more closely with the comprehensive provisions of the GDPR, policymakers should consider several key recommendations. Firstly, adopting more detailed and explicit provisions could provide greater clarity and protection for data subjects.

This involves outlining precise requirements for data subject rights, and how these rights can be exercised. In essence, this work is calling out for an amendment of the laws.

Secondly, it is crucial to implement checks and balances within a centralized enforcement system. For instance, establishing independent oversight mechanisms or board review could help mitigate the risk of potential abuse of power. These mechanisms should be designed to ensure that the centralized body operates transparently and is held accountable for its actions. Additionally, incorporating avenues for appeals and challenges could offer recourse for those affected by enforcement decisions, thereby enhancing the fairness and integrity of the enforcement process. These functions should be carried out by the courts to enhance adherence to the provisions.

5.4 Recommendations for Future Research

Future research should delve deeper into the practical impacts and effectiveness of different regulatory frameworks on data protection and privacy. An important area of investigation is the comparative effectiveness of decentralized versus centralized enforcement mechanisms. Research should explore how these mechanisms function in various regulatory environments and their influence on compliance, enforcement efficiency, and data subject rights protection.

5.5 Recommendations to enhance enforcement capabilities

To enhance enforcement capabilities, several measures can be taken:

Firstly, the foundation of effective enforcement lies in training and adequate resources. Data protection officers and enforcement personnel need access to detailed and up-to-date training programs preferably, free ones. These programs should cover a range of topics, from the intricacies of legal frameworks and emerging regulations to practical skills such as cybersecurity measures and investigative techniques.

Another critical component of strengthening enforcement capabilities is increasing public awareness. Educating the public about their data protection rights is essential for fostering a culture of compliance. Investing in advanced technological tools is another key strategy for improving enforcement capabilities. This includes automated systems that perform regular data protection audits can significantly enhance efficiency and accuracy. By adopting these recommendations, policymakers and enforcement bodies can strengthen data protection frameworks and ensure better protection for individuals' personal data.

5.6 OVERALL CONCLUSION

In conclusion, this work has served its purpose on the comparative analysis of the GDPR and NDPA in terms of data subject rights and privacy protection to uphold right to privacy. Throughout the work, a justification has been laid for the reason for the work and the need for a comparative analysis. This work further in chapter 2 and 3 rendered this analysis and in chapter 4 delivered its comparison. Finally, the work concluded with recommendations in chapter 5.

REFERENCES

Books

Akinsanya, A. A., & Ayoade, J. A. An Introduction to Political Science in Nigeria (2nd edn, University Press of America 2013).

McCullagh, K. Data Protection Law: Approaches to Privacy Governance in the EU and US (Cambridge University Press 2020).

Oluwole, O. Data Protection and Privacy in Nigeria: Law and Practice (University of Lagos Press 2021).

Oxford Learner's Dictionary (Oxford University Press 2020).

Voigt, P., & von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide (1st edn, Springer 2017).

Journal Articles

Achuonye, K. A. 'Digital Literacy and Primary Educational System in Nigeria' (2012) 3 Journal of Educational and Social Research 1.

Adediran, O., Oluwaseun, A., & Eze, S. 'The Evolving Landscape of Data Protection in Nigeria: Challenges and Opportunities' (2021) 7(1) African Journal of Law and Technology 89.

Adeyemi I, 'Enforcement Mechanisms of the GDPR and Their Application in Nigeria's NDPA: Lessons and Challenges' (2024) 12 ***Nigerian Journal of Law and Technology*** 45-63.

Agbakoba, O. 'Privacy Rights and Data Protection in Nigeria: Challenges and Prospects' (2022) 66(2) Journal of African Law 245-267.

Ajayi, G. O. 'Digital Literacy and the Challenges of Data Protection in Nigeria' (2020) 18(3) Journal of Information, Communication and Ethics in Society 345-360.

Ba-balola, O. ‘The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant’ (2024) 3 British Journal of Cyber Criminology 1.

Gonzalez, G., & Lamek, M. ‘GDPR Implementation Challenges’ (2018) 2(3) Journal of Data Protection & Privacy 203-218.

Goddard, M. ‘The EU General Data Protection Regulation (GDPR): European Regulation that Has a Global Impact’ (2017) 59(6) International Journal of Market Research 703-705.

Greenleaf, G. ‘Global Data Privacy Laws 2019: 132 National Laws & Many Bills’ (2018) 157 Privacy Laws & Business International Report 14-18.

Ifeoma, A. ‘The Illusion of Privacy in Social Media: An African Perspective’ (2013) 31 Journal of Information, Communication and Ethics in Society 251.

Iwu-James, J., James, T., & Iwu, C. ‘A Comparative Analysis of Data Protection Frameworks in Nigeria and the EU’ (2021) 5(2) Journal of International Data Privacy Law 45.

Ojo T, ‘The Nigerian Data Protection Act 2023: A Comparative Analysis with the GDPR’ (2023) 18 ***African Journal of Information and Communication Law*** 23-42**.**

Omrani, N., Schiavone, F., & Amir, C. ‘Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe’ (2024) Information Technology & People https://doi.org/10.1108/ITP-05-2023-0467 accessed 7 August 2024.

Olugbenga-Bello, A., Akande, T., & Eniola, A. ‘Data Protection Laws in Nigeria and the GDPR: A Comparative Study’ (2021) 3(4) Nigerian Journal of Data Protection and Privacy 112.

S. A. Oluwadare & F. A. Adebesin, ‘Data Protection in Nigeria: The Current State and Future Directions’ (2022) 12 Journal of Nigerian Law and Technology 45-67.

Reports and Publications

African Union Commission. The State of Data Privacy Laws in Africa (2019).

National Information Technology Development Agency. National Digital Literacy Framework (2019).

Nigerian Economic Summit Group. 'The State of Data Protection in Nigeria' (NESG Research Reports, 2021) 45-60.

United Nations Conference on Trade and Development. Digital Economy Report 2021 (United Nations 2021).

World Bank. Nigeria Digital Economy Diagnostic Report (World Bank Group 2020).

World Bank. Doing Business 2020: Comparing Business Regulation in 190 Economies (2020) World Bank Publications.

International Telecommunication Union. Measuring Digital Development: Facts and Figures 2020 (2020).

Legislations

Constitution of The Federal Republic of Nigeria

European Convention on Human Rights [1950] OJ 1 11.

General Data Protection Regulation [2016] OJ L119/1.

Nigerian Data Protection Act 2023.

Nigerian Data Protection Regulation

Case Law

British Airways Data Breach Case (2020) Information Commissioner's Office, available at https://ico.org.uk/about-the-ico/news-and-events/news-articles/british-airways-data-breach-fine/ (accessed 8 August 2024).

Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C: 2014:317.

Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020] ECLI:EU:C:2020:559.

Chapman v United Kingdom (2001) 33 EHRR 399.

Connors v United Kingdom (2004) 40 EHRR 189.

Dudgeon v United Kingdom (1981) 4 EHRR 149.

Digital Rights Lawyers Initiative & 2 Others v National Identity Management Commission & 1 Other [2020] Suit No AB/83/2020.

Gani Fawehinmi v Nigerian Bar Association [1989] 2 NWLR (HC) Pt 105, 558.

GC and Others v Facebook Ireland Ltd (C-136/17) [2019] EU:C: 2019:402.

Johnston and Others v Ireland (1986) 9 EHRR 203.

Keegan v Ireland (1994) 18 EHRR 342.

Liberty and Others v United Kingdom (2008) 48 EHRR 1.

Marckx v Belgium (1979) 2 EHRR 330.

NT1 & NT2 v Google LLC [2018] EWHC 799 (QB).

Nwabueze v Diamond Bank [2020] 3 NWLR 193.

Ojukwu v Governor of Lagos State [1986] 1 NWLR (FHC) Pt 18, 621.

Paradigm Initiative Nigeria & Ors v The Nigerian Communications Commission.

Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände (C-673/17) [2019] EU:C:2019:801.

Pretty v United Kingdom (2002) 35 EHRR 1.

Schwab v Facebook Ireland Ltd [2021] EWHC 1058 (QB).

Schrems v Data Protection Commissioner [2015] C-362/14 ECJ.

Ryneš v Úřad pro ochranu osobních údajů (C-345/17) [2017] EU:C: 2017:237.

S and Marper v United Kingdom (2008) 48 EHRR 50.

Uniqlo Co., Ltd v Spanish Data Protection Authority [2021] EWHC 2156 (Admin).

Regulatory Decisions

Commission Nationale de l'Informatique et des Libertés (CNIL), 'Sanction Pronounced Against Futura Internationale' (27 December 2018) Decision No SAN-2018-011.

Commission Nationale de l'Informatique et des Libertés (CNIL), 'Sanction Pronounced Against Google LLC' (21 January 2019) Decision No SAN-2019-001.

Irish Data Protection Commission, 'Decision on Inquiry IN-18-5-7' (31 December 2022).

Luxembourg National Commission for Data Protection (CNPD), 'Decision on Amazon.com Inc' (16 July 2021) Decision No 2021-009.

Additional Entries

European Union Agency for Fundamental Rights. Data Protection in the European Union: The Role of National Data Protection Authorities (2020).