UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 281-321
DOI: 10.47963/ucclj.v3i1.1259

DATA PROTECTION AND PRIVACY CHALLENGES IN NIGERIA: LESSONS FROM OTHER JURISDICTIONS

Patrick Chukwunonso Aloamaka[1]

ABSTRACT

Data protection and privacy challenges are prevailing issues in Nigeria and other developing countries in Africa. The crux of this paper is to examine the extent of the data and privacy challenges existing in Nigeria. Through a comparative analysis, this paper examined the existing provisions of data protection laws in some European countries and those of Nigeria with the aim of revealing the consequence of insufficient legislation to protect data or data users' privacy, the applicability and responsiveness of existing data protection laws in Nigeria, the dearth of legal precedents, the appalling lack of awareness of data privacy rights, and how it tends to handle or manage human rights violations. The paper adopts the doctrinal research method to identify these issues and propose viable solutions by comparatively examining the protection of data in Europe, with a focus on the legal regimes of data protection in the United Kingdom, Germany, and France. The paper concludes that Nigeria requires thorough data protection legislation like that of developed nations to provide effective data protection and a robust enforcement framework.

Keywords: Data Protection legislation, Privacy Challenges, General Data Protection Regulation, Nigeria Data Protection Regulation, Personal Data, NITDA

INTRODUCTION

In this era of technological advancements, the importance of data and privacy protection cannot be overstated. This paper aims to address the emerging challenges faced by data and privacy protection, particularly in Nigeria and other developing countries. It seeks to expose the extent of data protection and privacy challenges in Nigeria, analyse the existing

[1] Lecturer, Faculty of Law, Delta State University, Oleh Campus, Delta State, Nigeria. Email: barpataloa@gmail.com

provisions of data protection laws in Nigeria and selected European countries, highlight the consequences of inadequate legislation, assess the applicability of existing laws, identify the lack of legal precedents and awareness, and propose solutions through comprehensive data protection legislation.

While data protection regulations exist both nationally and internationally to safeguard users' data and privacy, loopholes still exist in Nigeria's regulatory framework. Traditional methods of data protection, such as paper forms and physical archiving, pose weaknesses, but resistance from individuals in traditional data storage roles also hinders progress.[2] The rise of cloud computing and remote access to data has displaced technology illiterate personnel.[3] Addressing these weaknesses is crucial for effective data protection and privacy measures.

The study also examines the practicability and responsiveness of existing legislation in handling breaches and explores the applicability of the General Data Protection Regulation in Nigeria. It considers the lack of judicial precedents and its impact on decision-making regarding data and privacy issues. Additionally, it recognizes the infringement of human rights caused by data invasion and intrusion,[4] citing examples such as loan rendering applications and the potential risks to applicants' data privacy if loans are denied.[5]

Drawing inspiration from Mark Zuckerberg's commitment to protecting users' Facebook data delivered on the 21st day in March 2018,[6] the study acknowledges the Nigerian Data Protection Regulation enacted in 2019 as an effort to address data safety concerns. The research methodology employed includes doctrinal and comparative analysis, allowing for

---

[2] Abiodun Odusote, 'Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation' (2021) 12(4) Beijing Law Review 1284.

[3] Junaid Hassan and others, 'The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR)' (2022) 2022 Computational intelligence and neuroscience 8303504 <https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=5c43590c-2cd5-4656-a476-a98f114b0cde%40redis> accessed 3 July 2023.

[4] Lee A. Bygrave, "Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements" (2017) 1 Oslo Law Review 105-120

[5] Kunle Sanni, 'INVESTIGATION: How Digital Loan Providers Breach Data Privacy, Violate Rights of Nigerians' (*Premiumtimesng.com*2021) <https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html?tztc=1> accessed 1 July 2023.

[6] Beryl A. Ehondor and Silk UgwuOgbu, "Personal Data Protection and Facebook Privacy Infringements in Nigeria" (2020) 17 Journal of Leadership, Accountability and Ethics

a comprehensive examination of data protection legislation in Nigeria compared to regulations in advanced countries.

Overall, this paper aims to shed light on the significance of data protection and privacy, identify challenges faced by Nigeria and other developing countries, and propose solutions through the adoption of robust data protection laws. It emphasizes the importance of safeguarding human rights, particularly the right to privacy, and draws insights from the experiences of first and second-world countries in shaping effective data protection measures.

THE LEGAL REGIME OF THE DATA PROTECTION IN NIGERIA

Even though the essence of data and its protection cannot be over-emphasized, the legal framework of data protection in Nigeria is somewhat fair compared to what was obtainable a couple of years back. Notwithstanding, several efforts have been made at diverse levels to make and enforce important provisions to help protect data retention and its use.

Although, there is insufficient legislation on the use and retention of data over the internet. However, as codified in Chapter 2 of the Constitution of the Federal Republic of Nigeria, the welfare and security of the people of Nigeria is one of the major duties of the government.[7] This is further backed by a provision of the same constitution which has specifically obliged the government of her duty to protect the privacy of her citizens. The General Data Protection Regulation adopted by the European Union applies to citizens of member countries as well as it provides for the export or transmission of data outside Europe. While the National Information Technology Development Agency (NITDA Regulation) and the Nigerian Data Protection Regulation were specifically designed to cater to data protection-related matters.

Therefore, this study will endeavour to analyse key provisions implemented in Nigeria regarding the utilization and storage of data.

[7] The 1999 Constitution of the Federal Republic of Nigeria as amended in 2011, s14(2)

The Constitution of the Federal Republic of Nigeria

Chapter IV of the Constitution of the Federal Republic of Nigeria being in relation to the subject matter, points at the provision of s37 thereof which provides for and avails every of its citizen the right to privacy.[8] This is of course the foundation of other data protection laws enforced in Nigeria.

The NITDA Regulation

The NITDA Regulation which was established pursuant to the NITDA Act gives powers to the Agency to make policies and guidelines for the safeguarding of data and to as well monitor the use of and exchange of data,[9] as stipulated in the far-reaching provision of s32 of the NITDA Act, capturing the NDPR under the same umbrella,

The Freedom of Information Act 2011 (FOIA)

As captured in section 14 of the FOIA, the provision clearly limits the power of the government from leaking personal data of any citizen except him/her consents to the disclosure. This is so to curtail and put to check the powers of the government, as they are saddled with the responsibility of being at the disposal of the personal data of citizens.

The Cybercrime Act (2015)[10]

With the pace at which the globe is becoming an internet-based space, this Act seeks to put internet service providers in check, as it spells out provisions for the protection of data of internet subscribers' right to privacy with the protection of their data and possible sanctions of the violation of this provision.

The Child Rights Act[11]

Nigeria enforced the Child Rights Act in 2003 according to the United Nations Convention treaty on the right of children was adopted to safeguard the rights and interests of children,

[8]Ali Toyin Smart, "An Examination of the Legal Framework for Data Protection in Nigeria and its Implications for Security And Economy", 2021
[9]Uche Val Obi SAN, "An extensive article on data privacy and data protection law in Nigeria | International Network of Privacy Law Professionals", 2020
[10] Cybercrimes (Prohibition, Prevention, ETC) Act, 2015
[11] Act No. 26 of 2003.

with s3 and s8 thereof, stipulating their fundamental rights and privacy respectively. Although these rights are put under the control of the child's parents or guardian.[12]

However, there are other minor regulations on the data subject, which include the Consumer Protection Council, The National Health Act (2014), the Anti-Discrimination Act 2014, and the likes of some other legislation that robs off on the subject of data protection.

With these been said, it is clear that NITDA regulations made a remarkable step towards the enforcement of data and privacy protection in Nigeria. It is plausible that Nigeria like a host of other countries did attempt to make better provisions using the GDPR as a guard, or yardstick to formulating useful data protection policies.[13]

CHALLENGES TO EFFECTIVE DATA PROTECTION IN NIGERIA

The major challenge posed by the effectiveness of data protection in Nigeria is basically attributed to non-enforcement and dearth of comprehensive and all-encompassing data protection laws and regulations. Unfortunately, the NDPR only applies to electronic data, leaving paper-based data infractions without recourse or protection.

Nigeria, being a developing country, faces challenges in terms of relying on traditional methods to protect data and the lack of adequate legislation to safeguard the privacy of data users. These traditional methods refer to activities like filling paper forms, filing documents, and archiving them in physical cabinets. However, it is important to note that one of the weaknesses does not lie in the data storage technology itself, but rather in the resistance exhibited by individuals who have been accustomed to the traditional role of data storage. This resistance may stem from a desire to avoid becoming redundant in the face of cloud computing data storage systems. It is important to address these weaknesses to ensure effective data protection and privacy measures in Nigeria.

However, reliance on section 37 of the Constitution has its own subtleties, particularly when dealing with a narrow-minded court, as we have seen in the past when clear cases of breach

[12]Ali Toyin Smart, "An Examination of the Legal Framework for Data Protection in Nigeria and its Implications for Security And Economy", 2021
[13]Uche Val Obi SAN, "An extensive article on data privacy and data protection law in Nigeria | International Network of Privacy Law Professionals", 2020.

of privacy have been dismissed because the court concerned opted to treat them as torts of nuisance.[14] To reach target markets and design campaigns, marketers have traditionally depended largely on customized data obtained from our internet habits and habits. They'll have to seek explicit permission to use personal data and be transparent about how they collect it in the future. Some in-house marketing teams and agencies may return to old marketing practices as a result of the changes and higher restrictions brought about by data protection legislation.

Furthermore, many websites do not charge their users to access their services, but they must pay to keep things running by selling user data to marketers. Some anticipate that sites may start charging for memberships and subscriptions in order to keep their website running without the free bandwidth.[15]

Nigeria has taken a firm stance in the fight against cybercrime, which has become a domestic and cross-border threat, with the introduction of the NITDA Regulation. It has established Nigeria as a legitimate member of the community of serious-minded nations dedicated to eradicating or at the very least minimizing the crippling effects of cybercrime on a variety of economies throughout the world. Security updates in networks, servers, and infrastructures, as well as other policy and security modifications, have been a main source of cyber protection until recently. The NITDA Regulation has had a direct impact on data privacy and security requirements, while also driving businesses to adopt and upgrade their cyber security procedures, reducing the danger of a data breach.[16]

A fundamental shift in the way businesses and individuals conduct business and interact with data in their possession while we've discussed how the landscape of this space might change in the post-NITDA Regulation period, we challenge the government to guarantee

---

[14] Olumide Babalola, 'Data Protection And Privacy Challenges In Nigeria (Legal Issues) - Privacy - Nigeria' (Mondaq.com, 2021) <https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-> accessed 13 August 2021.

[15]Uche Val Obi, SAN, 'An Extensive Article On Data Privacy And Data Protection Law In Nigeria | International Network Of Privacy Law Professionals' (International Network of Privacy Law Professionals, 2020) <https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/#:~:text=Breach%20of%20the%20privacy%20rights,of%20N10%20million%2C%20whichever%20is> accessed 13 August 2021

[16] Ibid

that its rules are adequately implemented. It will be possible to realize its promise if there is a strong enforcement mechanism in place to provide teeth to its provisions.[17]

Threat of improvement in information technology

It is needless to mention that in this era we are in, technology has been, and is excelling at the task of placing the world at our fingertips, so much so that virtually all and any information can be garnered at the comfort of our zones. This is of course not without its flaws as abusers have leveraged the vulnerability of these systems to support their deeds. The threats on the improvement of information technology to further enhance the circulation and retention of data are of course a matter of concern as it extends its tentacles to lack of adequate laws to completely deal with extant matters on the data subject. As there are only provisions of protection of digital data and no provisions for offline data, points out one of the major lapses of the existing data regulations, and also owing to the fact there are the dearth of decided cases on the subject matter.[18]

Insufficient legislation on the use and retention of data over the internet

A major problem faced by countries all over the globe on the subject of data protection, is not unknown, as various countries are yet to enact and enforce data and privacy protection legislation particularly in Nigeria.

As the world is beginning to wake up to the realization of the essence of data, there is a need for there to be matching rules to commemorate and then tackle issues arising from data. It is no longer news that several attempts have been made to replicate every single phase of the lots of human activities[19] and that has made the use and retention of data, particularly on users on the social media platforms.[20] This goes to tell more about why it is strongly advised that users and intending users read and understand the data and privacy protection policy before or during sign up, as users' data may be breached, exposed, and

[17] Ibid
[18]Olumide Babalola, 'Data Protection and Privacy Challenges in Nigeria (Legal Issues) - Privacy - Nigeria' (Mondaq.com, 2020) <https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-> accessed 25 July 2021.
[19]Uche Val Obi SAN, "An extensive article on data privacy and data protection law in Nigeria | International Network of Privacy Law Professionals", 2020
[20] Ibid.

then used by hackers to perpetrate evil. The exposure of personal variables such as names, addresses, age, and medical records in reported statistics is indeed a worrisome issue. Without proper legislation and safeguards in place, there are significant loopholes that can lead to the abuse of data and compromise individuals' vulnerability. Meanwhile, having to empower the NITDA Regulation to address data issues in Nigeria as NITDA Regulation makes a bulk of the landmark achievement of data and privacy protection in Nigeria. Having to create a practicable means to the enforcement of the provisions of the NITDA Regulations goes a long way to making the dream a reality.[21] Useful provisions can be coined from the AU's convention and the GDPR alike that spells out clearly how it is aimed at protecting citizen's data.[22]

Failures and malfunctioning of data technology hardware

Failures and the malfunctioning of data are no doubt fatal, as it is likely to cause loss of irretrievable data, which could be accidental or due to corruption or malfunctioning of the system. Hence, it is needless to mention here that failures of data hardware can amount to a loss of data. Amongst other things, data protection can also mean protection against hacking or corruption.[23] Fortunately, data protection strategy has reported data can likely be recovered or retrieved almost immediately after the loss or corruption.[24]

Failure of data technology sometimes can be attributed to invasion, by hackers surely because of lack of adequate data security. To make sure that the emerging internet-world becomes does not become vulnerable and to reduce the possibility of hacking, data

[21] Ibid.
[22]Emeka Ekweozor, 'An Analysis Of The Data Privacy And Protection Laws In Nigeria' [2020] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3639129#:~:text=There%20is%20presently%20no%20specific,of%20Nigeria%20(Promulgation)%20Act.> accessed 31 July 2021.
[23]Paul Crocetti, 'What Is Data Protection And Why Is It Important? Definition From Whatis.Com' (SearchDataBackup, 2021) <https://searchdatabackup.techtarget.com/definition/data-protection> accessed 31 July 2021.
[24] Ibid.

protection, and privacy should be given much attention, particularly as there are no sufficient laws that cover the entire spectrum of data and privacy.[25]

However, provisions to safeguard data on failed data tech hardware is a matter that requires urgent response and chances are that a decentralized system of operation may put an end to this, that is individuals can be left to placing restrictions on the usage of unencrypted private data rather leaving that to the tech companies to control.[26] In addition to addressing the issue of failed data tech hardware, it is crucial to consider implementing stringent measures to deter data breaches and ensure accountability. One effective approach could be the imposition of stiff and costly punishments that have the potential to financially cripple companies engaging in data misuse or negligence. Such penalties would serve as a strong deterrent and emphasize the importance of data privacy.

Furthermore, given the complex nature of technology and data privacy, it may be necessary to establish a specialized court comprising a new generation of judges who are well-versed in technology and data privacy matters. These judges would possess the expertise required to handle cases related to data breaches and privacy violations. This specialized court would provide a forum where legal matters pertaining to technology and data privacy can be addressed with a high level of understanding and competence.

This highlights the need for the establishment of robust enforcement agencies to ensure the effective protection and privacy of data. Additionally, legislative provisions and other necessary measures should be implemented to maximize data protection and privacy.

COMPARATIVE ANALYSIS OF DATA PROTECTION IN EUROPE

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a European Union law that went into effect in 2016 and, after a two-year transition period, became

[25]Camila Winlo, 'The 10 Data Privacy Fails Of The Decade – And What We Learnt From Them' (TechRadar, 2020) <https://www.techradar.com/uk/news/the-10-data-privacy-fails-of-the-decade-and-what-we-learnt-from-them> accessed 31 July 2021.
[26]Kurt Nielsen and Ana Alexandre, 'Tech Giants Failed To Protect Consumer Data — The Blockchain Can Help' (BeInCrypto, 2021) <https://beincrypto.com/tech-giants-failed-to-protect-consumer-data/> accessed 31 July 2021.

DOI: 10.47963/ucclj.v3i1.1259

directly applicable law in all European Union Member States on May 25, 2018, without necessarily requiring national law implementation by EU Member States.

THE UK LEGAL REGIME

The GDPR is preserved in domestic law as the UK GDPR, although the UK retains the authority to review the framework. The 'UK GDPR' coexists with an updated version of the Data Protection Act 2018. The government has released a Keeling Schedule for the GDPR in the United Kingdom, which details the changes.[27]

The fundamental concepts, rights, and obligations have not changed. 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in relation to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC' (General Data Protection Regulation)[28]

The GDPR's implementation is mostly determined by whether or not a company is based in the United Kingdom. An 'establishment,' as defined by the EU GDPR, can take many different forms and is not restricted to a firm established in the United Kingdom.[29]

The UK Data Protection Regulation applies to the processing of personal data that is done entirely or partially by automated means, as well as the processing of personal data that is done otherwise than by automated means and is part of or intended to be part of a filing system. The Data Protection Act of 2018 ("DPA") remains in effect as a national data protection law that supplements the GDPR regime in the United Kingdom. It deals with areas where derogations and exclusions from the EU GDPR were previously allowed (for

[27]'The UK GDPR' (Ico.org.uk, 2021) <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/> accessed 12 September 2021.

[28]'Regulation (EU) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA Relevance)' (Legislation.gov.uk, 2021) <https://www.legislation.gov.uk/eur/2016/679/contents> accessed 12 September 2021.

[29]Andrew Dyson and Ross McKean, 'Law In United Kingdom - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=GB&t=law#> accessed 12 September 2021.

example, substantial public interest bases for the processing of special category data, and context-specific exemptions from parts of the GDPR such as data subject rights).

Interestingly, the UK GDPR has extraterritorial impact and is based on the same principles as the EU GDPR. As a result, an organization that is not based in the United Kingdom will be subject to the UK GDPR if it processes personal data of data subjects in the United Kingdom where the processing activities are related to "the offering of goods or services" (Article 3(2)(a)) to such data subjects in the United Kingdom or "the monitoring of their behavior" (Article 3(2)(b)) as far as the processing activities are related to "the offering of goods or services" (Article 3(2)(a))[30]

Key Definitions

For support, an attempt will be made to outline some keywords under the UK GDPR. First, personal data as defined in Article 4 of the regulation is any information belonging to a natural person who can be identified. For this, a low bar has been established as regards telling what is identifiable. Personal data is information that can be used to identify a natural person using all reasonable means reasonably likely to be employed. Any identifier, such as an identity number, phone number, location data, or other information that could identify that natural person, may suffice.

The GDPR in the United Kingdom establishes stricter requirements for the processing of "special categories" (Article 9) of personal data (such as ethnicity, religion, sexual life, health, genetics, and biometrics) and personal data linked to criminal convictions and offences) (Article 10).

Apparently, the GDPR regulates the "processing" of personal data in the United Kingdom. Processing is a broad term that encompasses any collection of actions performed on data, including data storage, hosting, consultation, and deletion.

Secondly, the data subject is a natural person whose personal data is processed by either a controller.

[30] Ibid.

Thirdly, according to the provisions of the Article 4, the controller is the decision maker, the person who determines the goals and means of processing personal data, either alone or collectively with others. According to the controller's instructions, the processor processes personal data on behalf of the controller. In contrast to prior legislation, the GDPR places direct obligations on both the controller and the processor, while the processor has less obligations.

However, the DPA further emphasizes that where an enactment of law determines the purpose and means of processing, the person on whom the enactment imposes the responsibility to process the data is the controller.

Fourthly, in the UK GDPR, the terms public authority and public body are used. The DPA defines them in terms of the Freedom of Information Act 2000's concept of public authority.

Legal Regime

The GDPR is built around seven basic principles, which are outlined in Article 5 of the legislation and are intended to guide how people's data is managed. They don't operate as hard laws, but rather as an overall framework for laying out the GDPR's general objectives. The ideas are generally similar to those in prior data protection legislation.

Lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability are the seven principles of GDPR. Only one of these concepts, accountability, is new to data protection regulations.[31]

For support and reference purpose, Article 51 of the UK GDPR, provides that the Information Commissioner (whose powers are carried out by the Information Commissioner's Office (ICO) is the supervisory authority for the UK. The ICO no longer has any influence or membership in the European Data Protection Board as a result of Brexit, and it is no longer eligible to be nominated as a lead supervisory authority under the EU GDPR regime. This is reflected in the UK GDPR, which excludes Chapter 7 of the EU GDPR

[31]Condé Nast, 'What Is GDPR? The Summary Guide to GDPR Compliance in the UK' (WIRED UK, 2021) <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> accessed 12 September 2021.

DOI: 10.47963/ucclj.v3i1.1259

(Cooperation and Consistency) on the grounds that the UK will not participate in the EU's cooperation and consistency processes.[32]

Controllers and Processors' Obligations

Each controller or processor must appoint a data protection officer if it meets one or more of the following criteria under the UK GDPR:

It is a public authority; its core activities include processing operations that, by their nature, scope, or aims, necessitate large-scale regular and systematic monitoring of data subjects; or its core activities include large-scale processing of sensitive personal data.

Each use of personal data must be justified by reference to an adequate basis for processing in order to satisfy the lawfulness principle. Personal data may be handled on specific legal bases as spelt out in Article 6(1), also known as legitimate bases or lawful grounds.

Controllers and processors must ensure that the DPO is involved properly and in a timely manner in all issues relating to the protection of personal data Article 38(1), and the DPO must report directly to the highest management level, cannot be told what to do in the performance of his or her duties, and cannot be fired or penalized for doing so Article 38(3).

Also, Schedule 1 to the DPA adds to the standards for processing special categories of personal data and adds a number of "substantial public interest" reasons for processing special categories of personal data in specific settings regarded to be in the public interest. Many of these justifications are recognizable from prior UK law, while others are brand new.

Furthermore, the Article 39 clearly spells out and assigns tasks and functions of the data protection officers, which features; to inform and advise on GDPR and other UK data protection laws; to monitor compliance with the law and the organization's internal policies, including assigning responsibilities, raising awareness, and training staff; to advise and monitor data protection impact assessments when requested; and to cooperate and act as a point of contact with the supervisory authority.

[32] Ibid 3.

DOI: 10.47963/ucclj.v3i1.1259

Individual's Right

Individuals have the right to know what information the government and other organizations have about them under the Data Protection Act of 2018. These rights include the ability to:

Become aware of how their data is being used, how to gain access to personal data, and have inaccurate data amended, erasure of data, stop or limit the processing of their personal information. Portability of data (allowing them to get and reuse their data for different services), in certain cases, they have the right to object to how their data is processed.

Individuals also have rights when an organization uses your personal data for the following purposes: Decision-making processes that are automated (without human involvement); and profiling can be used to forecast an individual's data behaviour or interests, for example.

Enforcement

Just so to protect data subject, the UK GDPR did impose fines of up to 4% of annual global turnover, or GBP 17.5 million, by supervisory authorities (whichever is higher). Infringements of the basic principles for processing data, such as consent conditions and data subjects' rights, are subject to the maximum fines as deduced from the provision of Article 83(5).

In addition, the ICO has broad investigative and remedial powers, including the ability to conduct on-site data protection audits. The ICO's rights and obligations are outlined in Article 58 of the DPA. The ICO has the authority to perform a consensual audit of a controller or processor in order to determine if that organization is following best practices while processing personal data. However, the ICOs are not required to impose fines but to see to the enforcement of imposed sanctions or fines.

GERMAN LEGAL REGIME

In contrast to the Directive it replaced, a 'Regulation is directly applicable and has the same effect in all Member States. However, there are still more than 50 areas covered by GDPR where Member States can regulate differently under their own domestic data protection

legislation, and there is still an opportunity for differing interpretations and enforcement procedures among Member States.

Scope

The GDPR's implementation is mostly determined by whether or not a company is based in the European Union. An 'establishment' can take many different forms and isn't always a legal organization registered in one of the EU's member states.

The GDPR, on the other hand, has an extraterritorial impact. Even if an organization is not based in the EU, it will be subject to the GDPR if it processes the personal data of EU residents and the processing activities are related to the offering of goods or services just as codified in Article 3(2)(a) which may also imply that no payment is required to such EU residents, or the monitoring of their behaviour under the Article 3(2)(b) as far as their behaviour takes place.

The new German Federal Data Protection Act Bundesdatenschutzgesetz (BDSG) has updated Germany's legislative framework to comply with the GDPR. The BDSG was released on July 5, 2017 and went into effect on May 25, 2018, together with the GDPR. The goal of the BDSG is to take use of the GDPR's various opening clauses, which allow Member States to specify or even limit the GDPR's data processing requirements.[33]

There are a number of data protection standards in area-specific laws, such as those regulating financial trade or the energy sector, in addition to the BDSG. The Second Data Protection Adaptation and Implementation Act EU (ZweitesDatenschutz-Anpassungs- und Umsetzungsgesetz EU – '2. DSAnpUG-EU'), which went into effect on November 26, 2019, updated several of these regulations to the GDPR.[34] However, some particularly significant legislation, most notably the Telemediengesetz ('TMG'), have remained untouched, raising concerns about the future validity of the data protection requirements contained therein.

[33]Verena Grentzenberg, Dr. Jan Geert Meents and Jan Pohle, 'Law In Germany - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=DE&t=law#> accessed 13 September 2021.
[34] Ibid.

DOI: 10.47963/ucclj.v3i1.1259

Key Definitions

The definitions are the same as those found in Article 4 of the GDPR. Further definitions for 'public bodies of the Federation,' 'public bodies of the Länder,' and 'private bodies' can be found in Sec. 2 of the BDSG.

Firstly, the Federation's authorities, judicial bodies, and other public law institutions, as well as direct federal corporations, statutory organizations, and foundations founded under public law, and their affiliations, regardless of their legal form, are referred to as public bodies of the Federation.

Authorities, judicial bodies, and other public law institutions of a Land, a municipality, an association of municipalities, or other legal persons under public law subject to Land supervision, and their associations, regardless of their legal form, are referred to as public bodies of the Länder.

Regardless of the participation of private bodies, associations of public bodies of the Federation and the Länder founded under private law and performing public administration functions shall be recognized as public bodies of the Federation. They operate outside of a country's borders, or the Federation owns or controls the absolute majority of shares or votes in the country. Otherwise, they will be treated as Länder public bodies.

Unless they are covered by subsections 1 to 3, private bodies are natural and legal persons, societies, and other associations founded under private law. If a private body performs sovereign administrative functions for the government, it is a public body as defined by this Act.

If the Federation's public bodies compete as enterprises governed by public law, they are considered private bodies as specified in this Act. If they compete as firms governed by public law and carry out federal legislation, and if data protection is not managed by Land law, public bodies of the Länder are also considered private bodies as specified in this Act.

Legal Regime

Germany been the first EU member state to pass a Data Protection Adaptation and Implementation ActBundesdatenschutzgesetz (BDSG). It is then needless to mention that

the GDPR has been the primary data protection legislation since 2018, and it has greatly aided in the harmonisation of data protection laws among EU member states. Furthermore, the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und Informationsfreiheit – 'BfDI') serves as the Data Protection Authority for telecommunication service providers and represents Germany in the European Data Protection Board. A group comprised of members from all public and private sector authorities - the 'Data Protection Conference' (Datenschutzkonferenz 'DSK') – was established to ensure that all authorities have the same attitude. The consistency system under the GDPR is modelled after the German authorities' coordination framework.

Controllers and Processors' Obligations

The Act covers the processing of personal data by public and private bodies, as well as other federal data protection legislation. It applies to all data that is processed by natural persons in the course of a purely personal or domestic activity. The (EU) 2016/679 and Parts 1 and 2 of the Act applies accordingly to the processing of personal data by public bodies in the context of activities outside the scope of Regulation (EU) 2016/679 and Directive (EU)20.

The bar for the appointment of DPOs in Germany is far lower than that set out in the GDPR. Amongst their several functions, controllers and processors must ensure that the DPO is involved "properly and in a timely manner in all issues relating to the protection of personal data" Article 38(1), and the DPO must report directly to the highest management level, cannot be told what to do in the performance of his or her duties, and cannot be fired or penalized for doing so Article 38(3).[35] Also, if the controller or processor conducts processing that is subject to a data protection impact assessment pursuant to Art. 35 GDPR, or if they commercially treat personal data for the purposes of transfer, anonymized transfer, or market or opinion research, a DPO must be designated.

Just as in the case of most other jurisdiction, unless the data subject releases him or her from this responsibility, the DPO is bound by secrecy regarding the identity of data subjects

[35] Ibid.

and situations that enable data subjects to be identified. In addition, the DPO has the authority to refuse to give evidence in specific circumstances.

A data subject's complaint shall be directed to the lead supervisory authority in the Land where the controller or processor has its main establishment, as defined in Article 4 no. 16 of Regulation (EU) 2016/679, or its single establishment in the European Union. If no agreement can be reached, the method outlined in Section 18 (2) will be followed.

Interestingly, the German authorities demand that the DPO speaks the same language as the competent authorities and data subjects, i.e. German, or that immediate translation be provided.

Individual's right

Data subjects have a variety of rights regarding the processing of their personal data, some of which are quite broad in scope and others that apply only in very specific circumstances. Controllers are required to disclose information on actions done in response to requests within one calendar month by default, with the controller having a limited ability to extend this period by two months if the request is onerous.

Access to information as engraved in Article 15, shows that data subject has the right to seek access to and a copy of his or her personal data, as well as prescribed information about how the controller has used the data.

As clearly stated in Article 16 of the GDPR, data subjects have the right to have erroneous or incomplete personal data repaired or updated as soon as possible.

As deduced from Article 17 of the Act the right to erasure is sometimes known as the right to be forgotten Data subjects have the right to have their personal data erased. In 2014, Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), effectively ordering Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google, as the data controller of the search results, had no legal basis to process that information. Although, this right is not absolute; it only applies in a limited set of circumstances, such as when the controller no longer requires the data for the purposes for which they were collected or otherwise lawfully

processed, or as a result of the controller's successful exercise of the right to object or withdraw consent.

The data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used, and machine-readable format where the processing of personal data is justified either on the basis of the data subject's consent to processing or where processing is necessary for the performance of a contract (eg, commonly used file formats recognized by mainstream software applications, such as .xsl).[36]

Additional rules apply to the processing of particular categories of personal data under the BDSG. In some situations, contrary to Art. 9 (1) GDPR, public and private organisations may process such data; see Sec. 22 (1), 26 (3) BDSG. In addition, Sec. 24 BDSG establishes the circumstances in which controllers may treat data for purposes other than those for which the data were obtained.

In Section 26 of the BDSG, special rules apply to processing for employment-related purposes. The German legislator has made extensive use of Art. 88 (1) GDPR's opening clause, thus establishing a separate employee data protection system.

Enforcement

Data protection regulators, also known as supervisory authorities, are in charge of enforcing the GDPR for example, the CNIL in France or the Garante in Italy. The European Data Protection Board the successor of the so-called Article 29 Working Party is made up of delegates from supervisory authorities who monitor the GDPR's implementation across the EU and issue advice to encourage consistent interpretation.

Germany does not have a single Data Protection Authority, but rather a number of separate Authorities for each of the 16 German states (Länder) that are in charge of enforcing data protection laws and regulations. Furthermore, the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und

[36] Ibid.

Informationsfreiheit – 'BfDI') serves as the Data Protection Authority for telecommunication service providers and represents Germany at the European Data Protection Board.

The repression the German authorities stated that fines will be computed not just on the turnover of the single concerned company, but also on the turnover of the entire group of companies. However, in Germany, whether this interpretation of Art. 83 (4), (5), and (6) GDPR in relation to Recital 150 GDPR is correct is now hotly debated, with strong arguments against it. The Act on Regulatory Offences (GesetzüberOrdnungswidrigkeiten – 'OWiG') governs the enforcement of penalties; additional sanctions, such as a temporary or permanent limitation or prohibition on processing, are governed by administrative procedures.[37]

FRENCH LEGAL REGIME

With the enactment of Law No. 2018-493 of June 20, 2018 on the protection of personal data, and Order No. 2018-1125 of December 12, 2018, adopted pursuant to Article 32 of Law No. 2018-493, France updated Law No. 78-17 of January 6, 1978 on information technology, data files, and civil liberties (the "Law") to GDPR. The issuance of Decree No. 2019-536, enacted for the application of the Law (the "Decree"), completed France's domestic data protection legislation.

Scope

Article 3 of the Law currently states that it applies whether I the data controller or data processor is based in France (regardless of whether the processing takes place there) or (ii) the targeted data subjects reside in France. It goes without saying that enterprises founded in any EU member state are subject to the GDPR's regulations. Furthermore, if any EU resident's data is involved, as well as if they monitor the behavior of EU residents, the GDPR may apply to firms founded outside of EU states.

[37] Ibid.

Key Definitions

The definitions in the law are identical to those in the GDPR. Article 2 of the Law expressly refers to GDPR definitions, bringing French legal definitions and concepts in line with the GDPR.

The essential principles that apply to the French data protection regulation clearly specify that data gathered must be processed in accordance with the stated out standards, just as they do with the GPDR. It must also be done in accordance with the law. This means that the processing must be done in accordance with EU data protection legislation. Furthermore, the legal bases are spelled forth in detail in Article 6.

Personal data can be acquired for a variety of reasons, including valid ones as well as clear and specified ones. It must be kept up to date and safeguarded. The data controller should be held responsible for adhering to the data protection principles.

Legal Regime

Act No. 78-17 on Information Technology, Data Files, and Civil Liberties, enacted on January 6, 1978, as amended by Act No. 2018-493 on Personal Data Protection, enacted on June 20, 2018, which: incorporates certain provisions of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data.[38]

Controllers and Processors' Obligations

Personal data must be treated in a secure manner that protects it against unauthorized or unlawful processing, as well as accidental loss, destruction, and damage. Both controllers and processors must ensure that they have the necessary technical and organizational mechanisms in place to comply with the GDPR's requirements. This is depending on the security risk, which could include personal data encryption, the ability to maintain the

[38]Myria Saarinen and others (Lw.com, 2021) <https://www.lw.com/thoughtLeadership/data-protection-in-france-overview> accessed 13 September 2021.

DOI: 10.47963/ucclj.v3i1.1259

continuous confidentiality, integrity, and resiliency of processing systems, and other factors.[39]

Individual's right

A data subject has the right to file a complaint about their personal data with the Commission Nationale Informatique & Libertes (CNIL) if an infringement occurred in France or the data subject is a resident of France, as stated in the GDPR.

Furthermore, the data subject has the right to request or demand a copy of the personal data that has been processed or gathered. Unless they have already received all necessary information, data subjects must be informed about how personal data will be handled at the time the data is collected, according to Article 13 of the GDPR. Furthermore, data subjects must be informed of their right to specify criteria for the processing of their personal data after their death, according to Article 32 of the DPA.

Enforcement

Inspections should be carried out on-site. Members of the CNIL, with the exception of private houses, have access to places, facilities, or equipment used for processing personal data for professional reasons from 6 a.m. to 9.00 p.m. The public prosecutor must be notified in advance, as well as the person in charge of the private professional premises, of their right to object to the inspection. If they oppose, the visit will be allowed only with the permission of the liberty and custody judge. However, if the visit is warranted by urgency, the gravity of the circumstances, or a risk of destruction or concealment of documented evidence, it can be made without notifying the person in charge of the premises and with the judge's permission. The person in charge cannot oppose to the visit in this circumstance. The visit must be conducted under the authority and control of the liberties and custody judge who authorized it, in the presence of the occupant of the premises or his or her representative, who may be assisted by a counsel of his or her choice, or in the presence

[39]BorianaGuimberteau and Clemence Louvet, 'Data Protection 2021 | Laws And Regulations | France | ICLG' (International Comparative Legal Guides International Business Reports, 2021) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/france> accessed 13 September 2021.

of two witnesses who are not placed under the authority of the persons in charge of the inspection.[40]

Execute additional control procedures. The CNIL can, for example, consult data on an online communication service to the public that are freely accessible or made accessible, including through negligence, imprudence, or third-party actions, if necessary by accessing and maintaining an automated data processing system for the duration of the operation. The CNIL has the authority to record data in any suitable manner in documents that are readily available for control purposes. CNIL agents can employ a fictitious identity to conduct any online activity required to carry out their task. Except for material protected by attorney-client privilege, the protection of journalistic sources, or medical confidentiality, CNIL agents are not subject to secrecy (Article 44, DPA; Article 65-1, DPA Decree). Submit formal requests for document or file communication. Carry out hearing tests.

Following the enactment of the Consumer Protection Act of 2014, the CNIL has been empowered to undertake online inspections (looking at any publicly available information, such as online privacy policies, online consent processes, and cookie compliance).

Impeding the CNIL's actions (by refusing to carry out the CNIL's obligations, refusing to provide the information and documents requested, or providing inaccurate information) can result in a year in prison and a EUR15,000 fine Article 51, DPA. Since the Digital Republic Law was enacted, the CNIL's chairwoman has been able to initiate summary proceedings for required remedies in circumstances of serious and imminent infringement of data subjects' rights and freedoms (Article 52, DPA).[41]

[40]Myria Saarinen and others (Lw.com, 2021) <https://www.lw.com/thoughtLeadership/data-protection-in-france-overview> accessed 14 September 2021.
[41] Ibid.

UCC Law Journal. Volume 3 Issue 1 Jul. 2023, pp. 281-321
DOI: 10.47963/ucclj.v3i1.1259

THE LEGAL FRAMEWORK FOR DATA PROTECTION IN NIGERIA

Nigeria is yet to establish comprehensive data protection and privacy legislation. However, privacy and data protections are included in a number of proposed and enacted sector-specific regulations.

Despite significant progress in recent years, Nigeria still lacks a dedicated primary data protection legislation. In fact, until the National Information Technology Development Agency (NITDA) established its Data Protection Regulation in early 2019, data protection protections in general and sector-specific legislation were scarce, ineffective, and fragmented. The Regulation aims to protect natural persons' right to privacy, promote the safe conduct of transactions involving the interchange of personal data, prevent personal data manipulation, and keep Nigerian firms competitive.[42] Policies to control data protection are in place, and most of the time they are based on the assumption that it is a right that comes with a responsibility to comply.

Nigerian people have a fundamental right to privacy under the Nigerian Constitution. Citizens' privacy in their residences, mail, telephone conversations, and telegraphic communications is guaranteed by Section 37 of the Constitution. The term "privacy" is not defined in the Constitution, and there are no specific privacy provisions. Electronic media, including as mobile devices and the Internet, are covered by the Constitutional right to privacy. Violations of these rights could result in civil penalties.

All mediums through which Personal Data is gathered or processed must display a straightforward and noticeable privacy policy that is easily understood by the intended Data Subject class, according to the NITDA Regulations.[43]

In Nigeria, the National Information Technology Development Agency (NITDA) is the primary data protection regulator. Sector-specific regulatory bodies, such as the Nigerian

[42]Ademola Adeyoju, 'A Quick Guide On The Data Protection Regime In Nigeria' [2020] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522188> accessed 13 August 2021.
[43]Sandra Oyewole, 'Law In Nigeria - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=NG&t=law#> accessed 13 August 2021.

Communications Commission and the Central Bank of Nigeria, provide data protection services.

The Regulation applies to all transactions involving the processing of personal data relating to natural persons residing in Nigeria or outside Nigeria who are citizens of Nigeria. To achieve its goals, provisions are made in the far-reaching regulation, as it lays forth the foundations for lawful data processing and requires anybody who collects, uses, stores, or processes personal data to follow particular guidelines. Some of the regulations as earlier discussed will be reiterated for support;

The Child Rights Act of 2003 reaffirms children's constitutional right to privacy. Section 8 of the Act provides a child's right to privacy, subject to the right of the parent or guardian to supervise and manage their child's behaviour. Child Rights Laws have also been implemented in some Nigerian states.

The Cybercrimes (Prohibition, Prevention, and Punishment) Act establishes a legislative and regulatory framework in Nigeria for prohibiting, preventing, detecting, prosecuting, and punishing cybercrime. The Act makes it illegal to intercept electronic communications and requires financial institutions to keep and secure data.

The Nigerian Communications Commission (NCC) issued the NCC Regulations, which require all licensees to take reasonable precautions to protect customer information from improper or unintentional exposure, as well as to guarantee that it is securely stored and not held for longer than is necessary. The NCC Regulations further prohibit the sharing of customer information to any third party unless the Customer has agreed to it or the NCC or other applicable laws or regulations approve or require it.

The Central Bank of Nigeria Act of 2007 was used to implement the Consumer Protection Framework of 2016. Financial institutions are prohibited from sharing personal information about their consumers under the Framework. Financial institutions must also have suitable data protection procedures and employee training programs in place to prevent unauthorized access, alteration, disclosure, unintentional loss, or destruction of customer data, according to the Framework. Before sharing personal data with a third party or using it for promotional purposes, financial services providers must get written consent from customers.

The Credit Reporting Act creates a legal and regulatory framework for credit bureaus to report on their customers. Credit Bureaus are required by Section 5 of the Credit Reporting Act to keep credit information for at least 6 years from the day it is collected, after which it must be preserved for a 10-year period before being destroyed. Data subjects (i.e. people whose credit data is stored by a credit bureau) have the right to privacy, confidentiality, and protection of their credit information under Section 9 of the Credit Reporting Act. Section 9 further specifies the circumstances under which credit information about data subjects may be provided.

The Freedom of Information Act (FOIA) aims to protect personal information. A public institution is required by Section 14 of the FOI Act to decline any application for information including personal information unless the individual involved consents to the disclosure or the information are publicly available. A public institution may decline an application for disclosure of material that is subject to certain forms of professional privilege given by law, according to Section 16 of the FOI Act (such as lawyer-client privilege, health workers-client privilege, etc.).

The National Identity Management Commission (NIMC) was established by the NIMC Act to establish and maintain a National Identity Management System (NIMS). The National Identity Management Commission is in charge of registering citizens and legal residents, building and administering a National Identity Database, and providing Unique National Identification Numbers to qualifying citizens and legal residents. No person or corporate body shall have access to data or information contained in the Database with respect to a registered individual without consent from the Commission, according to Section 26 of the NIMC Act. The Commission has the authority to transfer information recorded in an individual's Database entry to a third party without the individual's agreement, as long as it is in the public interest.

The Bill's principal goal is to establish a framework for the protection of personal data and to control the processing of information about all individuals, regardless of country. It also aims to defend the constitution-guaranteed fundamental rights to privacy and liberties. The bill is still being reviewed and may be altered further before becoming law.

On February 6, 2019, the Federal Competition and Consumer Act of 2019 were signed into law. The Commission is required by Section 34(6) of the Act to protect the business secrets

of all parties involved in Commission investigations. Hearings before the Commission are required to be held in public under Section 33(2), however, the Commission may hold hearings in-camera for a variety of reasons, including the preservation of corporate secrets.

Telephone subscriber records kept in the NCC's central database are kept confidential under Sections 9 and 10 of the NCC Regulation 2011. Telephone subscribers also have the right to examine and update personal information maintained by the NCC in a telecommunication company's central database.

The Nigerian Data Protection Regulation Implementation Framework (the Framework) was recently approved and distributed by the National Information Technology Development Agency (NITDA). To ensure a targeted application of the data protection regime in Nigeria, the Framework relies on the Nigeria Data Protection Regulation 2019 (NDPR). It is intended to help data controllers and administrators/processors understand the standards that must be met in order for their organizations to be compliant. The Framework should be read in conjunction with the NDPR, not in place of it.[44]

Scope

As captured in Part One of the Nigerian Data Protection Regulation 2019, the regulation says, among other things, it applies to all transactions involving the processing of personal data. Regardless of the means by which data processing is carried out or is planned to be carried out in relation to natural people in Nigeria.

Key Definition

Personal data is defined as any information about a living person who can be identified. An identifiable natural person is one who can be identified, either directly or indirectly, using an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity. Personal data is a broad word that includes information such as a person's name, address, photo, email address, bank account information, social

[44] Ibid.

DOI: 10.47963/ucclj.v3i1.1259

networking website posts, medical information, and other unique identifiers such as MAC and IP addresses, IMEI numbers, SIM cards and others.

An identifiable natural person is referred to as a data subject. An identifiable natural person is one who can be identified, either directly or indirectly, using an identifying number or one or more elements unique to his physical, physiological, mental, economic, cultural, or social identity.

A Data Controller is a person who, alone, jointly or in common with others, or as a statutory authority, determines the purposes for which and how Personal Data is or will be processed.

A breach of security that results in unintentional or unlawful destruction, loss, modification, unauthorized disclosure, or access to Personal Data transmitted, stored, or otherwise processed is referred to as a Personal Data Breach.

Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure through transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction are all examples of processing.

Controllers and Processors' Obligations

Personal Data must be collected and processed for a specified, reasonable, and lawful purpose that the Data Subject has consented to. However, the basic obligation of the controllers and processors of data in Nigeria is to provide continual capacity building for its DPOs and all workers involved in any type of data processing as deduced from Section 4.1(3) of the NDPR.

Secondly, they are obliged to ensure that data subjects' consent was obtained without fraud, coercion, or undue influence. This is stated in Section 2.3(2) of the NDPR. They must also send a soft copy of the audit summary containing information about processed data to NITDA if it processes more than 1,000 data subjects in a six-month period. See Section 4.1(6) of the NDPR; and submit a summary of its data protection audit to NITDA if it

DOI: 10.47963/ucclj.v3i1.1259

processes more than 2,000 data subjects in a 12-month period by 15 March of the following year (Section 4 of the NDPR)[45].

Individual's Right

The NITDA Regulation outlines the Data Subject's rights in detail, including the minimum requirements for processing personal data, the Data Subject's right to be informed of appropriate data protection safeguards, the Data Subject's right to request deletion of personal data in appropriate cases, and a reiteration of the protection of fundamental rights provided by the GDPR.

Enforcement

NITDA has the authority to register and license Data Protection Compliance Organizations that monitor, audit, train, and consult with all Data Controllers under the Regulation on behalf of NITDA. NITDA is also required to establish an administrative redress panel that will (a) investigate allegations of any violation of the Regulation's provisions, (b) invite any party to respond to allegations made against it within seven days, (c) issue administrative orders to protect the subject matter of the allegation pending the outcome of the investigation, and (d) conclude investigations and make appropriate recommendations. A violation of the Regulation is considered a violation of the NITDA Act of 2007. Any licensee who violates any of the Regulations would be in violation and subject to the fines, sanctions, or penalties that the Commission may impose from time to time.[46]

Despite the fact that the NDPR authorizes NITDA to sanction data controllers and processors who violate its provisions, NITDA has yet to use its sanctioning powers against any data controllers or processors.[47]

---

[45]Akinkunmi Akinwunmi, 'Nigeria - Data Protection Overview' (DataGuidance, 2021) <https://www.dataguidance.com/notes/nigeria-data-protection-overview> accessed 14 September 2021.
[46]Sandra Oyewole - DLA Piper Global Data Protection Laws of the World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=NG&t=law#> accessed 13 August 2021.
[47]Akinkunmi Akinwunmi, 'Nigeria - Data Protection Overview' (DataGuidance, 2021) <https://www.dataguidance.com/notes/nigeria-data-protection-overview> accessed 14 September 2021.

DOI: 10.47963/ucclj.v3i1.1259

Analysis of the General Data Protection Law

Data protection rules must regulate and influence the operations of enterprises and governments in modern societies in order to empower us to control our data and protect us from abuses. These institutions have repeatedly demonstrated that unless regulations constraining their behaviour are in place, they will try to collect everything, mine everything, keep everything, and share it with others while informing us of anything. Meanwhile, Nigeria currently lacks a formal or comprehensive data privacy or protection law. In contrast to Nigeria, Data protection rules must regulate and influence the operations of enterprises and governments in modern societies in order to empower us to control our data and protect us from abuses. However, the GDPR introduces additional restrictions on how consent is obtained and how children's data is processed, while the reasons for processing personal data remain mostly unchanged. As a result, consent in data collection is now subject to stricter regulations.[48]

There are certain limitations on the use of legitimate interests as a basis for processing, as well as some clarification on when this can be done. When deciding whether the processing of data for a new purpose is incompatible with the original purposes for which the data was obtained, there is a non-exhaustive list of elements to consider.

[48]Sara Owens, General Data Protection Regulation (GDPR) - Gap Analysis (Adaptation Of Document Courtesy Of Sara Owens, Information Compliance & Knowledge Manager At The Solicitors Regulation Authority) (2021) <https://www.whatdotheyknow.com/request/405995/response/983183/attach/8/GDPR%20Gap%20Analysis.pdf?cookie_passthrough=1> accessed 14 September 2021.
S6(1)(f) Is required for the protection of legitimate interests
Public authorities processing personal data in the course of their duties can no longer rely on this ground.The new GDPR defines "data subject consent" as "any freely given, precise, informed, and unequivocal expression of his or her desires by which the data subject, either by a statement or by a clear affirmative action, expresses approval to the processing of personal data relating to them."
"Ticking a box when visiting a... website, choosing technical settings... or any other statement or conduct that clearly indicates... the data subject's agreement of the proposed use of their personal data," according to Recital 25. As a result, silence, pre-ticked boxes, or inactivity should not be construed as consent." Unless additional regulatory requirements (such as provision of care where consent is implied/life or death, etc.) apply, explicit consent is still necessary to justify the processing of sensitive/special categories of personal data.

The current Act does not specify any restrictions on how children's data may be used, and the rules for how minors can consent have been taken from national laws. The most significant child-related provision is Article 8, which stipulates that any information society services offered directly to a child under the age of 16 must have parental consent. However, a Member State may lower this age limit to 13 and it only applies when processing is based on the child's consent.

According to GDPR Article 8(1a), the controller must additionally use "reasonable efforts" to confirm that consent has been given or approved by the person with parental responsibility.[49] To uniquely identify a person, novel biometric and genetic data were analyzed (new). Surprisingly, for GDPR reasons, information related to criminal convictions and transgressions is not regarded as "sensitive."

According to the GDPR, data about criminal convictions and offences may only be processed when under the direction of an official authority or when permitted by Union or Member State law that includes the essential safeguards.[50] When processed "to uniquely identify a person," "special categories of personal data" now expressly include "genetic data" and "biometric data."

The GDPR's grounds for processing sensitive data are similar to those in the present Act, albeit there are several exceptions in the area of health and healthcare management. Member States also have a broad capacity to impose new restrictions (including prohibitions) on the processing of health data, biometric or genetic.[51]

CONCLUSION

In conclusion, the NITDA Regulation represents a significant step towards modernizing Nigeria's data privacy and protection legislation, mirroring the impact of the GDPR on global privacy law and policy. This article has demonstrated how various countries worldwide have embraced the principles embodied in the GDPR and incorporated them into their domestic

[49] Ibid.
[50] Ibid.
[51] Ibid.

laws, including Nigeria's adoption of the NITDA Regulation, which introduces substantial changes to the existing framework. Moving forward, we can expect a transformation in the way businesses and individuals handle and interact with the data they control or retain. While this piece has explored the potential changes that may arise in the post-NITDA Regulation era, the effectiveness of the regulation will largely depend on robust implementation and enforcement. A strong enforcement framework, supported by stringent measures, will be instrumental in ensuring that the regulation fulfils its intended purpose. Overall, the NITDA Regulation presents an opportunity for Nigeria to enhance data privacy and protection practices. By aligning with internationally recognized standards, Nigeria can pave the way for improved data governance and contribute to the broader global efforts in safeguarding personal information.

RECOMMENDATIONS

For effective data protection, Nigeria must enact a comprehensive and thorough data protection legislation.[52] When significant legislation, as opposed to a 'supplemental regulation', is enacted, a country is considered to be treating data privacy seriously.[53] One can argue that the Regulation (NDPR) is fairly thorough in that it covers important concerns such as data privacy and security, which could help to curb harmful data practices and prevent data abuse by data controllers and processors. More so, personal data must be used in conformity with the reason for it collection. Prior to collecting personal data, the individual's consent must be sought. For example, the EU GDPR and other national data privacy regulatory authorities have made it unlawful for their individual and corporate residents to transmit or disclose data gathered within their borders to countries that have lax or no data privacy legislation.[54]

---

[52] Olayinka Alao, 'Nigeria: The Nigeria Data Protection Bureau and the Challenges of Data Privacy Compliance in Nigeria' (*www.mondaq.com*30 March 2022) <https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-dataprotection-bureau-and-the-challenges-of-data-privacy-compliance-in-nigeria> accessed 24 February 2023.

[53] Patrick Chukwunonso Aloamaka, 'EFFECTIVE DATA PROTECTION in NIGERIA: CHALLENGES' (2022) 8 Commonwealth Law Review Journal 660 <https://thelawbrigade.com/wp-content/uploads/2022/11/Patrick-Chukwunonso-Aloamaka-CLRJ.pdf> accessed 10 January 2023.

[54] Ibid.

A specific Data Protection Directive for all national security agencies should be included in the data protection reform, just so to establish standards for the transmission of personal data at national and international levels.

The public should be made aware of the NDPR's provisions as well as the significance of protecting data privacy.[55] The goal of the sensitization campaigns should be to educate both data subjects and data processors about their rights and the repercussions of breaking the NDPR.[56] Working together with traditional media outlets or social media is one way to do this as the effectiveness of data privacy protection will increase as a result.[57]

The physical hazards of hardware failure and data technology failure must be protected against when handling data.[58] Given that users may be the root of a system's failure, users are essential in preventing system failure.[59] The two greatest methods for preventing system failure are code testing and user manuals that include system specifications.[60]

REFERENCES

Adelola, Tiwalade, Ray Dawson, and Firat Batmaz, "Nigerians' Perceptions of Personal Data Protection and Privacy", 2015.

Adeyoju A, 'A Quick Guide On The Data Protection Regime In Nigeria' [2020] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522188> accessed 13 January 2023.

[55] Ibid.
[56] Ibid.
[57] Ufuoma V Awhefeada and Ohwomeregwa Ogechi Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (2020) 8 Journal of Law and Criminal Justice 30.
[58] Ibrahim Shehu and Sani Rabiu Bello, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria' (2022) 121 Journal of Law, Policy and Globalization 54.
[59] Ibid.
[60] Muli David Tovi and Mutua Nicholas Muthama, 'Addressing the Challenges of Data Protection in Developing Countries' (2013) 1 European Journal of Computer Science and Information Technology 6 <https://www.eajournals.org/journals/european-journal-of-computer-science-and-information-technology-ejcsit/vol-1-issue-2-september-2013/addressing-the-challenges-of-data-protection-in-developing-countries/> accessed 24 February 2023.

Akinwunmi A, 'Nigeria - Data Protection Overview' (*One Time Data Guidance*28 May 2021) <https://www.dataguidance.com/notes/nigeria-data-protection-overview>

Akinwunmi A, 'Nigeria - Data Protection Overview' (DataGuidance, 2021) <https://www.dataguidance.com/notes/nigeria-data-protection-overview> accessed 14 September 2022.

Alao O, 'Nigeria: The Nigeria Data Protection Bureau and the Challenges of Data Privacy Compliance in Nigeria' (*www.mondaq.com*30 March 2022) <https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-dataprotection-bureau-and-the-challenges-of-data-privacy-compliance-in-nigeria> accessed 24 February 2023.

Ali TS, 'An Examination of the Legal Framework for Data Protection in Nigeria and Its Implications for Security and Economy' (*The IP Press*22 July 2021) <https://www.theippress.com/2021/07/22/an-examination-of-the-legal-framework-for-data-protection-in-nigeria-and-its-implications-for-security-and-economy/> accessed 2 March 2023.

Aliyu, Abubakar Sanni, "THE NIGERIA DATA PROTECTION BILL: APPRAISAL, ISSUES, AND CHALLENGES" (2016) 9 Innovative Issues and Approaches in Social Sciences.

Aloamaka PC, 'EFFECTIVE DATA PROTECTION in NIGERIA: CHALLENGES ' (2022) 8 Commonwealth Law Review Journal 660 <https://thelawbrigade.com/wp-content/uploads/2022/11/Patrick-Chukwunonso-Aloamaka-CLRJ.pdf> accessed 10 January 2023.

Anic I, Škare V, and Kursan Milaković I, 'The Determinants And Effects Of Online Privacy Concerns In The Context Of E-Commerce' (2019) 36 Electronic Commerce Research and Applications.

Awhefeada UV and Bernice OO, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (2020) 8 Journal of Law and Criminal Justice 30.

Babalola O, 'Data Protection and Privacy Challenges in Nigeria (Legal Issues) - Privacy - Nigeria' (Mondaq.com, 2020) <https://www.mondaq.com/nigeria/data-

protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues-> accessed 25 July 2022.

Bamberger K, and Mulligan D, 'Privacy In Europe: Initial Data On Governance Choices And Corporate Practices' (2013) 81 George Washington Law Review <https://ssrn.com/abstract=2328877> accessed 12 August 2021.

Bygrave, Lee A., "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements" (2017) 1 Oslo Law Review.

Crocetti P, 'What Is Data Protection and Why Is It Important? Definition from Whatis.Com' (SearchDataBackup, 2021) <https://searchdatabackup.techtarget.com/definition/data-protection> accessed 31 July 2022.

Crutzen R, Ygram Peters G, and Mondschein C, 'Why and How We Should Care About The General Data Protection Regulation' (2019) 34 Psychology & Health.

Custers B and others, 'A Comparison of Data Protection Legislation and Policies across the EU' (2018) 34 Computer Law & Security Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091040> accessed 10 August 2022.

Custers B and others, 'Informed Consent In Social Media Use – The Gap Between User Expectations And EU Personal Data Protection Law' (2013) 10 SCRIPTed <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047134> accessed 10 August 2022.

Custers B, van der Hof S, and Schermer B, 'Privacy Expectations Of Social Media Users: The Role Of Informed Consent In Privacy Policies' (2014) 6 Policy & Internet <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047163> accessed 10 August 2022.

Da Veiga A, and Ophoff J, 'Concern For Information Privacy: A Cross-Nation Study Of The United Kingdom And South Africa' [2020] Human Aspects of Information Security and Assurance.

'Data Protection' (GOV.UK, 2021) <https://www.gov.uk/data-protection> accessed 9 August 2022.

Dyson A, and McKean R, 'Law In United Kingdom - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=GB&t=law#> accessed 12 September 2022.

Ehondor, Beryl A., and Silk Ugwu Ogbu, "Personal Data Protection and Facebook Privacy Infringements in Nigeria" (2020) 17 Journal of Leadership, Accountability and Ethics.

Ekong, Iniobong, Emeka Chukwu, and Martha Chukwu, "COVID-19 Mobile Positioning Data Contact Tracing and Patient Privacy Regulations: Exploratory Search of Global Response Strategies and the Use of Digital Tools in Nigeria" (2020) 8 JMIR mHealth and uHealth.

Ekweozor E, 'An Analysis of the Data Privacy and Protection Laws in Nigeria' [2020] SSRN Electronic Journal.

Ekweozor E, 'An Analysis Of The Data Privacy And Protection Laws In Nigeria' [2020] SSRN Electronic Journal.

'Enforcement Action' (Ico.org.uk, 2021) <https://ico.org.uk/action-weve-taken/enforcement/> accessed 10 August 2022.

Garbis, Jason, and Jerry W. Chapman, "Data Protection" [2021] Zero Trust Security.

'GDPR' (Itgovernance.co.uk, 2021) <https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation> accessed 10 August 2022.

Grentzenberg V, Meents D, and Pohle J, 'Law In Germany - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=DE&t=law#> accessed 13 September 2021.

'Guide To Data Protection' (Ico.org.uk, 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/> accessed 10 August 2022.

Guimberteau B, and Louvet C, 'Data Protection 2021 | Laws And Regulations | France | ICLG' (International Comparative Legal Guides International Business Reports, 2021) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/france> accessed 13 September 2021.

Hainsdorf C and Liard B, 'Data Protection Laws and Regulations France ' (*International Comparative Legal Guides*2019) <https://iclg.com/practice-areas/gambling-laws-and-regulations/singapore> accessed 13 March 2023.

Hassan J and others, 'The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges-A Systematic Literature Review (SLR)' (2022) 2022 Computational intelligence and neuroscience 8303504 <https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=5c43590c-2cd5-4656-a476-a98f114b0cde%40redis> accessed 3 July 2023.

Idepefo, Felix Olutokunbo, Bernard Ijesunor Akhigbe, Ojo Stephen Aderibigbe, and Babajide Samuel Afolabi, "Towards an Architecture-based Ensemble Methods for Online Social Network Sensitive Data Privacy Protection" (2021) 9 International Journal of Recent Contributions from Engineering, Science & IT (iJES).

'Law In France - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?t=law&c=FR> accessed 13 August 2022.

Leone N, 'Think Privacy Is Not Important and You've Got Nothing to Hide' (*www.linkedin.com*2021) <https://www.linkedin.com/posts/nelioleone_kwara-technology-tedx-activity-6798113905840336896-a0tl> accessed 2 March 2023.

Leone, Nelio, "Think Privacy is not important and you've got nothing to hide?" (https://www.linkedin.com/posts/nelioleone_kwara-technology-tedx-activity-6798113905840336896-a0tl 2021).

Mrabure, Kingsley Omote and Ufuoma Veronica Awhefeada, 'Onnoghen's Cjn Conundrum, Exercise of the Executive Powers of the President and the Practice of Separation of Powers in Nigeria' (2020) 46 Commonwealth Law Bulletin 440

<https://doi.org/10.1080/03050718.2020.1756878> accessed 3 February 2023.

Nast C, 'What Is GDPR? The Summary Guide To GDPR Compliance In The UK' (WIRED UK, 2021) <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> accessed 12 September 2021.

Nielsen K, and Alexandre A, 'Tech Giants Failed To Protect Consumer Data — The Blockchain Can Help' (BeInCrypto, 2021) <https://beincrypto.com/tech-giants-failed-to-protect-consumer-data/> accessed 31 July 2021.

Obi SAN, Uche Val, "An extensive article on data privacy and data protection law in nigeria | International Network of Privacy Law Professionals", 2020.

Odusote A, 'Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation' (2021) 12 Beijing Law Review 1284.

Olawunmi I and Emejuo CC, 'An Examination of the Legal Framework for Data Privacy and Protection in Nigeria' [2021] SSRN Electronic Journal.

Owens S, 'Data Protection Officer Appointment - a Freedom of Information Request to Gloucestershire Care Services NHS Trust' (*WhatDoTheyKnow*11 May 2017) <https://www.whatdotheyknow.com/request/405995/response/983183/attach/8/GDPR%20Gap%20Analysis.pdf?cookie_passthrough=1> accessed 4 March 2023.

Owens S, General Data Protection Regulation (GDPR) - Gap Analysis (Adaptation Of Document Courtesy Of Sara Owens, Information Compliance & Knowledge Manager At The Solicitors Regulation Authority) (2021) <https://www.whatdotheyknow.com/request/405995/response/983183/attach/8/GDPR%20Gap%20Analysis.pdf?cookie_passthrough=1> accessed 14 September 2022.

Oyewole S, 'Law in Nigeria - DLA Piper Global Data Protection Laws of the World' (*www.dlapiperdataprotection.com*2021) <https://www.dlapiperdataprotection.com/index.html?c=NG&t=law#> accessed 4 March 2023.

Oyewole S, 'Law In Nigeria - DLA Piper Global Data Protection Laws Of The World' (Dlapiperdataprotection.com, 2021) <https://www.dlapiperdataprotection.com/index.html?c=NG&t=law#> accessed 13 August 2021.

'Regulation (EU) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation) (Text With EEA Relevance)' (Legislation.gov.uk, 2021) <https://www.legislation.gov.uk/eur/2016/679/contents> accessed 12 September 2021.

Saarinen M and others (Lw.com, 2021) <https://www.lw.com/thoughtLeadership/data-protection-in-france-overview> accessed 14 September 2021.

Sanni K, 'INVESTIGATION: How Digital Loan Providers Breach Data Privacy, Violate Rights of Nigerians' (*Premiumtimesng.com*2021) <https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html?tztc=1> accessed 1 July 2023.

SHEHU I and BELLO SR, 'Challenges to the Implementation and Enforcement of Data Protection in Nigeria' (2022) 121 Journal of Law, Policy and Globalization 54.

Smart, Ali Toyin, "An Examination of the Legal Framework for Data Protection in Nigeria and its Implications for Security And Economy", 2021.

'The UK GDPR' (Ico.org.uk, 2021) <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/> accessed 12 September 2021.

Tovi MD and Muthama MN, 'Addressing the Challenges of Data Protection in Developing Countries' (2013) 1 European Journal of Computer Science and Information Technology 6 <https://www.eajournals.org/journals/european-journal-of-computer-science-and-information-technology-ejcsit/vol-1-issue-2-september-2013/addressing-the-challenges-of-data-protection-in-developing-countries/> accessed 24 February 2023.

Winlo C, 'The 10 Data Privacy Fails Of The Decade – And What We Learnt From Them' (TechRadar, 2020) <https://www.techradar.com/uk/news/the-10-data-privacy-fails-of-the-decade-and-what-we-learnt-from-them> accessed 2 March 2023.

Wu P, Vitak J, and Zimmer M, 'A Contextual Approach To Information Privacy Research' (2019) 71 Journal of the Association for Information Science and Technology.

STATUTES

Constitution of the Federal Republic of Nigeria 1999 (As Amended)

Child Rights Act 2003

Consumer Code of Practice Regulations 2007 (NCC Regulations)

Consumer Protection Framework 2016 (Framework)

Credit Reporting Act 2017

Cybercrimes (Prohibition, Prevention Etc) Act 2015

Data Protection Act, 2018 of the United Kingdom

Data Protection Bill 2019 (the Bill)

Freedom of Information Act, 2011 (FOI Act)

Federal Competition and Consumer Protection Act, 2019

Implementation Framework for the Nigeria Data Protection Regulation

National Identity Management Commission (NIMC) Act 2007

National Information Development Technology Agency (NITDA) Act

National Health Act 2014 (NHA)

DOI: 10.47963/ucclj.v3i1.1259

Nigerian Communications Commission (registration of telephone subscribers) Regulation 2011

Nigeria Data Protection Regulation 2019