Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Area Six

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Data Privacy and Protection: Technical Components of Regulations and Implications for Cybersecurity Risk Management Practices

Talabi, A.A., Longe, O.B, Muhammad, A.A. & Olusanya, K.
[1]Doctoral Candidate, African Centre of Excellence for Technology Enhanced Learning (ACETEL)
National Open University of Nigeria, Abuja, Nigeria
[2]Faculty of Computational Sciences & Informatics, academic city University, Accra, Ghana
Department of Computer Science, Kaduna State University, Kaduna, Nigeria
Industry Expert from ISACA, Ibadan, Oyo State, Nigeria
E-mail: doyin.talabi@gmail.com; olumide.longe@acity.edu.gh; muhdaminu@kasu.edu.ng; kunlesanya2002@gmail.com

ABSTRACT

The world is largely interconnected through the internet and users generate 2.8 quintillion bytes of data daily. This high volume of data has attracted cybercriminals who hack systems to get access to personal data, steal identity, corrupt data with fire consequences to individuals, groups, organisations and governments. To control the use of personal data, many countries and regions have promulgated data privacy regulations to control the collection and use of personal data. The National Information Technology Development Agency (NITDA) put in place the Nigeria Data Protection Regulation (NDPR) effective January 2019 and all organisations and public sector institutions are to comply. This paper reviewed the NDPR to highlight the technical requirements and recommend appropriate cybersecurity management practices to put in place for compliance and ensure data protection and privacy. The paper concluded that awareness about the need for data privacy and protection is growing. All organisations, both in the public and private sectors, should keep abreast of NDPR provisions, requirements and put in place appropriate technical controls and policies to avoid negative consequences including fines and loss of reputation and disruption of operations due to unauthorized access resulting in exposure of personal data of data subjects.

Keywords: Data protection, data privacy, nigeria data protection regulation, personal data

Proceedings Citation Format
Talabi, A.A., Longe, O.B, Muhammad, A.A. & Olusanya, K. (2022): Data Privacy and Protection: Technical Components of Regulations and Implications for Cybersecurity Risk Management Practices. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022.
Pp 107-112. www.isteams.net/ecowasetech2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P20

1. INTRODUCTION

The world has become a global village enabled by the internet and internet-based technologies. Many people utilize technology tools and platforms like electronic email, blogs, websites, portals, social media sites and mobile apps to send, receive, access and share information at a high speed irrespective of geographical distance. According to Statista (statista.com, 2022), a website that tracks internet statistics[1], 4.6 billion out of the 7.9 billion estimated world population (about 58%) are active internet users and 4.2 billion are active social media users as at January 2021.

This large population of active users generate a lot of data daily and this has been estimated at about 2.5 quintillion bytes (18 Zeroes) of data daily. According to next-tech.com (next-tech.com, 2022) [2] , this figure will increase with the adoption of Artificial Intelligence (AI), Machine Intelligence (ML) and Internet of Things (IoT) technologies. This heightened use of the internet, social media and mobile applications that generate data create cybersecurity risks and vulnerabilities that may be exploited by cybercriminals, either as a single entity, in groups or even by government sponsored agents. Cyber-attacks have become common and successful have resulted in financial, reputation and business losses, according to cyberdb.com (cyberdb.com,2022) [3]. This necessitates that Cybersecurity risks that must be managed appropriately at personal, group, organizational and government levels. Cloudfare(cloudflare.com, 2022) [4] defines data privacy as that which concerns the protection of the personal data of individuals and defines who is authorized to gain access to such information, while data protection refers to the actions and controls put in place to safeguard the information from unauthorized access, theft or corruption (techtarget.com,2022) [5], according to techtarget.com.

Many countries including Nigeria, Ghana, China, South Africa and the European Union have enacted Data Privacy and Protection regulations to guide personal data management practices in their jurisdiction. Under the NDPR, personal data refers to “Any information that relates to an identified or identifiable living individual e.g., BVN, NIN, email, IP address, location, medical data, fingerprints, staff number, date of birth, driving license number, mother’s maiden name, etc.”. Sensitive Personal data refers to “racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data or biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation” (nitda,2021) [6] and this is stated in the NDPR implementation toolkit released by the National Information Technology Development Agency (NITDA)

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/

[2] https://www.the-next-tech.com/blockchain-technology/

[3] https://www.cyberdb.co/financial-cyber-attacks-in-2021

[4] https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-privacy

[5] https://www.techtarget.com/searchdatabackup/definition/data-protection

[6] https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

2. METHODOLOGY

This paper carried out a systematic review of the Nigeria Data Protection Regulation (NDPR) to highlight its principles, guidelines and achievements since inception. It also highlighted technical components and its infrastructure and control implications for cybersecurity management practices in organisations.

2.1 Review Of The NDPR

The Nigeria Data Protection Regulation (NDPR) was promulgated by the National Information Technology Development Agency (NITDA) in 25 January 2019 and applies to all organisations, whether in the public or private sector that process the personal data of residents of Nigeria, as well as Nigerian citizens abroad [6]. The NDPR sets out rules and regulations, guidelines, requirements and sanctions for non-compliance. The objectives of the NDPR include safeguarding the rights of natural persons to data privacy, preventing manipulation of Personal Data, fostering safe conduct for transactions involving the exchange of Personal Data, and ensuring that Nigerian businesses remain competitive in international trade through the safeguards afforded by a data protection regulatory framework that is in line with global best practice.

According to NITDA, the principles of NDPR include that personal data to be processed must be collected lawfully and for legitimate purpose, must be accurate and adequate, secured and stored only for the period for which it is needed. The personal data can only be processed after getting consent of the owner, in the performance of a contract or is a legal obligation, performance of a task in public interest or in the vital interest of the owner, referred to as a data subject in NDPR.

Major requirements of the NDPR that have implications for Information Technology infrastructure and controls and cybersecurity management practices are discussed below.

a. **Data Minimization** – Data Controllers and (organizations that determines how data will be processed) or process data on behalf of others (Data Administrators) are required to ensure that they only collect minimum data required as agreed with the data subject.
b. **Storage and Retention periods** – Data controllers must ensure that personal data is kept only for the period for which it is reasonably required
c. **Confidentiality, Integrity and Availability** – Data Controllers must comply with basic standards of information security management
d. **Appointment of DPO and DPCO** – All data controllers must appoint data protection officers (DPO) for their organisations and employ NITDA registered Data Protection Compliance Organisations (DPCO) as their external consultants and perform their annual statutory data unit and send their annual audit reports through such DPCOs.
e. **Data Privacy Notice and Data Privacy Policy** – All Data Controllers are required to have data privacy policy on every medium through they collect personal data i.e. on websites, in publications and displayed conspicuously in organisation's premises
f. **Data Protection Compliant systems** – All systems and applications that would process personal data must be built with data privacy in mind during project design
g. **Data Breach Notification** – Notify the regulator, NITDA of any known data breach within 72 hours of becoming aware of that breach

h. **Data Subject Access to Personal Data** – Data controllers are to design systems to ensure that data subjects can access, modify and delete information subject to agreed terms and conditions
i. **Use of Cookies** – Use of cookies on websites or any digital platform requires consent
j. **Annual Data Audit** – Data Controllers must carry out annual audits on or before 15th March of every year
k. **Data Transfers Abroad** - Any data transfers abroad must be done in accordance with the provisions of the NDPR
l. **Data Retention Period** – Every data controller/ administrator must state clearly its duration of storage in the contract or binding document
m. **Sanction for Non-compliance** - Penalty attracts up to N10 million or 2% of the company's annual global revenue of the preceding year; whichever is higher.

2.2 NDPR Performance Statistics

According to a performance report published by the Nigeria Data Protection Bureau (NDPB) on the NDPR for 2020-2021(NDPB,2021) [7] , it has recorded some modest achievements since 2019, despite the economic shutdown in 2020 due to COVID-19 related issues. Tables 1and 2 provide a comparison of 2020 and 2021 figures.

Table 1: NDPR Performance Statistics

ITEM	2020	2021
Audits Filings received	635	1,229
Jobs created	2,686	7680
Data Breaches investigated	15	17
No of Investigations concluded	1	7
No of Issues resolved	790	2080
Amount of fines issued	1m	15m
No of People Trained	N/A	5,746
Revenue to Govt. from filing	18.5m	24.5m
No of Licensed Privacy Consultants	70	103
Values of NDPR Data Audit Market	2.2Billion	1.8Billion
Phone Calls Received by NITDA	1,230	1,350
No of Economic Sectors involved	13	20
Others	Truecaller service was made to review its privacy policy	Twitter service was engage and made to comply with the NDPR

[7] https://www.ndpb.gov.ng/Files/hhNITDA_Compiled NDPR Draft 2020-2021_0701.pdf

Table 2: Analysis of Number of Audits Filed by Sector

NO	SECTOR	2020	2021
1	Financial Services + Insurance	220	536
2	Consultancy and others	54	121
3	ICT and Media	55	109
4	Manufacturing/FMCG	92	98
5	Energy/Oil and Gas	65	86
6	Health	26	55
7	Transport, Maritime, Aviation and Logistics	33	54
8	Public sector	17	49
9	Mining and Extractive	6	33
10	Agriculture	29	26
11	Construction + Engineering	9	16
12	Trade & Education	7	15
13	Real Estate	22	7

3. DISCUSSION OF RESULTS

An analysis of the performance statistics indicates an increasing level of awareness about the NDPR. For example, the number of audit reports filed increased from 635 to 1,229, 5,746 people were trained, 7,680 jobs created as against 2,686 in 2020. The number data breaches reported and being investigated increased from 15 to 17, number of issues resolved increased from 790 to 2080 indicating increase awareness. Government revenue also increased from 18.5 million Naira to 24.5 Million. The financial sector had the highest number of compliant organisations, followed by the Consultancy sector while the ICT and media sector, was third. The Manufacturing sector was fourth, followed by the Energy/Oil and Gas sector, while the health sector was sixth. The Public sector and the Trade and education sectors seem to be slow adopters.

4. RECOMMENDED CYBERSECURITY MANAGEMENT PRACTICES

The technical components highlighted above require technical controls and procedures to be put in place to assure cybersecurity and protection of digital assets(dporganizer,2022) [8].

These controls include

a) Regular cybersecurity and data privacy and protection awareness training
b) Creation of access control list and password levels
c) Installation and use of antivirus software with regular updates
d) Encryption and Pseudonymisation of personal data stored
e) Physical security controls like access key, use of biometrics and CCTV installation
f) Information security policies including password policies, data protection policy, data retention policy, data disposal policy, privacy policies and notices
g) Personnel Background checks for sensitive positions
h) Regular data risk assessments and audit
i) Disaster Recovery and Business Continuity planning

[8] https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/

CONCLUSION

Data privacy concerns the proper handling and protection of personal data for confidentiality purposes and also ensures compliance with legal regulations such as the NDPR. Putting cybersecurity controls and information security best practices in place will protect brand reputation, avoid financial losses and ensure operations continuity for organisations. Awareness about the need for data privacy and protection is growing. All organisations, both in the public and private sectors, should keep abreast of NDPR provisions, requirements and put in place appropriate technical controls and policies. This would help to avoid contravention, fines and loss of reputation, finance, legal issues and disruption of operations due to unauthorized access resulting in exposure of personal data of data subjects. Educational institutions in particular must put in place secured collection, transmission and storage processes and technologies when handling documents like admission lists, examination results, medical examination results and transcripts that include personal data

REFERENCES

[1] https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed25/2/2022)
[2] https://www.the-next-tech.com/blockchain-technology/ (Accessed25/2/2022)
[3] Cyberdb.com. financial cyberattacks. (2022) https://www.cyberdb.co/financial-cyber-attacks-in-2021/ (Accessed25/2/2022)
[4] Clouflare.com what is data privacy (2022). https://www.cloudflare.com/en-gb/learning/privacy/what-is-data-privacy/(Accessed25/2/2022)
[5] Techtarget.com data protection (2022). https://www.techtarget.com/searchdatabackup/definition/data-protection (Accessed25/2/2022)
[6] nitda.gov.ng NDPR Implementation framework (2021). https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf Accessed25/2/2022)
[7] ndpb.gov.ng. NDPR Performance Report 2020-2021. (2022). https://www.ndpb.gov.ng/Files/hhNITDA_Compiled NDPR Draft 2020-2021_0701.pdf (Accessed 27/4/2022)
[8] dporganizer.com organizational measures (2022)] https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/ (Accessed24/2/2022)