DIGITAL TRADE PROTECTIONISM IN NIGERIA UNDER THE NIGERIAN DATA PROTECTION ACT 2023: LESSONS FROM EUROPEAN UNION

Olumuyiwa Bankole, B.A (ed) English Language,
Ekiti State University, Ado-Ekiti, Nigeria

ABSTRACT

Digital trade governance in Nigeria is still novel and significantly leverages on data collections, analyses and processes into policy decisions. Nigeria historically migrated into data governance in 2023 upon enactment of the Data Protection Act, aligning domestic data regulation with the global standards. However, the strict provisions of data localization and sector-specific restriction of cross-border data transfers have enabled *de facto* digital trade protectionism hobbling Nigeria's commitments to the regional digital trade captured under the AfCFTA Digital Trade Protocol. This paper critically analyses ways the Data Protection Act supports protectionism, evaluates its impact on digital trade, and glean lessons from the European Union's GDPR towards enhancing digital market integration and liberalization. The paper reveals that the Nigeria Data Protection Act 2023 invents digital trade protectionism in the pattern of sector-specific data localization, and restrictive data transfer, undermining digital trade liberalization and limiting the expansion of Nigeria's digital economy which should naturally thrive on multilateralism or trade freedom. The paper therefore proposes an EU Model of harmonizing its interoperability instruments—adequacy decisions, standards contractual clauses, and risk-layered data localization--with the NDPA 2023 to achieve its AfCFTA obligations and unwind its digital trade for global competition.

Keywords: Digital Trade, Protectionism, Data Protection Act and EU.

I. Introduction

Digital trade ecosystem is fast emerging in Nigeria following the significant global transition to digital economy and wealth creation[1]. The world digital trade market export was to the threshold of $7.23 trillion as at 2024 which represents $2.64 trillion increase from the year 2020 digital trade export at the rate of 12.1% annual growth, faster than entire global trade estimate by 9.7% and keeps growing in an accelerated manner than global trade evaluation[2]. Advanced economies, particularly the European Union (EU), the United States, and the United Kingdom, were the leading countries. The emerging markets including India, China, and Brazil were also growing in their own pace[3]. As at 2024, digital trade market represents 25% global economy. This estimates shows the significant contribution of digital trade to the overall global economy.

The developed economies like European Union and UK have long embraced digital trade and built context-specific regulatory frameworks around it as a reflection of their jurisdictional or regional needs[4]. The EU states like Spain, Germany, Italy, and France among others have unified and mature data-aligned digital trade regulatory framework, the GDPR 2019. The United Kingdom which exited the Union still adopts the GDPR with other aligned UK-specific frameworks to enhance seamless operation of the GDPR to regulate its data-aligned digital trade in a liberal and sustainable pathways[5]. Germany, Spain Italy and France do not have any separate national data laws but operates within the EU GDPR and Digital Single Market Framework[6].

Nigeria is the largest economy in Africa, a strong member of the African Union and African Continental Free Trade Agreement (AfCFTA) and signatory to the AfCFTA Protocol on Digital Trade 2024[7]. Nigeria is gradually growing its digital market including its fintech

---

[1]JAMMY. Digital technology and the economic transformation of Nigeria via the lens of Delta State: opportunities, challenges, and future prospects. *Rowter Journal,* Vol.4, n4, 2025 pp.1-15. DOI: 10.33258/rowter.v4i1.1235

[2]UNCTAD Data Hub. Digital economy and technology Data insights

[3] PIOTR. Emerging Markets as Key Drivers of the Global Economy. *European Research Studies Journal*. Vol. 26, n4 pp. 431-445. DOI: 10.35808/ersj/3294

[4]World Investment Report. Chapter IV: International investment in the digital economy (2025). https://unctad.org/system/files/official-document/wir2025_ch04_en.pdf

[5] EU Commission Publication. Legal framework of EU data protection

[6] Syed Hassan. The Impact of EU GDPR on the Digital Economy of EU (The document is shared subject to Copy Rights of the Author and require explicit prior permission before using any parts of this document). DOI: 10.13140/RG.2.2.29528.75521

[7] ADETOYE. Nigeria and the African Continental Free Trade Agreement Area (AFCFTA): Issues, Challenges and Prospect. *Advances in Social Sciences Research Journal*, Vol. 7, n 2, 2020, pp. 237-250.

ecosystems and up-scaling its digital infrastructures to compete with global digital business space[8]. This came into reality when it enacted its Data Protection Act in 2023 as legal framework to regulate all data-aligned digital businesses in Nigeria and outside as it relates to global privacy practices and cross-border data governance[9].

This paper significantly identifies data protectionism as a significant barrier to global digital trade caused by regulatory frictions under the NDPA 2023 spanning cross border data transfer barrier, sector-specific data localization, conflict with the AfCFTA prohibition of data-aligned digital market localization, shrinking economic policy impact and mis-alignment with patentable multilateral digital trade principle canvassed by the World Trade Organisation . The provisions of the NDPA 2023 are pro-digital trade protectionism strictly localizing data governance and limiting the Nigerian positive digital trade impact on global e-commerce, cloud and digital trade services through restriction of cross-border data transfer.

At a time, the EU states experienced the same challenges while developing their Digital Single Market as a region. The EU states had to comprehensively enact the GDPR in the context of EU digital market and proactively align it with mechanism that prompt data flows[10]. The EU states finally integrated unique components of data flows including adequacy decisions, standard contractual clauses and interoperability procedures into the GDPR framework for seamless implementation of digital trade in alignment with the WTO rules on multilateralism[11]. Hence, the EU states have opened their multilaterally aligned digital businesses and e-commerce to countries around the world and expand their revenue generation to be among the top-tiered threshold[12].

The paper reveals that Nigeria legal framework aligns with digital trade protectionism with strong restrictions on cross-border data transfer and localization of data governance which

DOI: 10.14738/assrj.72.7698

[8]OLUWASEMILORE. Challenges of Nigeria's digital economy: Way forward. *UCC Law Journal*. Vol.3, n. 1, 2023, pp. 229-260 DOI: 10.47963/ucclj.v3i1.1257

[9] AHMED and MUHAMMAD. Assessing the adoption of Nigeria Data Protection Act (2023): A case study of some selected higher institutions in North-Eastern Nigeria. *Open Journal of Physical Science,* Vol. 6, n 2, pp. 14-25. DOI:10.52417/ojps.v6i2.921

[10]Gilbert and Gilbert. Impact of General Data Protection Regulation (GDPR) on Data Breach Response Strategies (DBRS). doi.org/10.47772/IJRISS.2025.914MG0061

[11]Martina and Bernard et al. Digital trade, data protection and the EU adequacy club. *Economica*, Vol. 93, n 369, 2025, pp. 230-259. DOI: 10.1111/ecca.70016

[12]Herman and Maria-Ana. Can EU Countries Balance Digital Business Transformation with the Sustainable Development Goals? An Integrated Multivariate Assessment. *Systems,* Vol. 13, 2025, pp. 722. https://doi.org/10.3390/ systems13080722

significantly hinder digital trade liberalism and seamless multilateral e-commerce interoperability. These limitations serious dwindle investments in digital trade ecosystems in Nigeria and restrict Nigeria's vision for multilateralism in digital trade.

The paper, therefore, proposes the EU dual-Model of harmonizing strong data privacy and open digital trade governance mechanism for Nigeria. The EU states deployed adequacy decisions by aligning and mobilizing standard contractual clauses (SCCs), risk-layered localization system to enhance multilateral digital trade system. Deploying this model will build Nigeria's capacity to fulfil its e-commerce obligations under the AfCFTA Digital Trade Protocol 2024 which implements regional digital trade liberalization. The EU Model will also strengthen open Nigeria to multilateralism-modelled digital investments and economic profits. The components of this paper analyse Nigeria's digital trade protectionism governance, evaluate its trade and economic impacts, and glean significant lessons from the EU Model to promote Nigeria's digital trade openness and investments.

2. Legal Framework for Business-aligned Data Governance in Nigeria

2.1.Digital Trade under the Nigerian Data Protection Regulation 2019

Historically Nigerian data governance commenced with the subsidiary legislation made to regulate personal data in 2019 when the Nigerian Data Protection Regulation was issued. In response to stakeholder clamour for legal framework for data governance, the National Information Technology Development Agency ("NITDA) issued a subsidiary instrument captured Nigerian Data Protection Regulation 2019 (the "Regulation"). This piece of Regulation set regulated the processing of private data relating to Nigerian citizens living in Nigeria or living outside Nigeria[13]

However, the scope of the Regulation did not contemplate artificial person or corporate entities, it was specific on natural persons alone. The decided case of *Olumide Babalola Esq V. Soko Lending Company Limited*[14] instituted pursuant to Articles 2.2, 2.5, and 3.1(7) of the NDPR and relevant section 37 of the Nigerian 1999 Constitution elicited the gap of data-aligned artificial person. The case was strictly decided on privacy rights of a Nigerian. His Lordship,

[13] Nigerian Data Protection Regulation, s. 1(2)
[14] LD/13031MFHR/2022 (Unreported)

E.O Ashade decided that,

> The Respondent lacked the legal basis for processing the Applicant's personal data (especially their name and telephone number) to send the Applicant unsolicited and offensive WhatsApp messages…the Respondent's privacy policy published on its website as of February 1, 2022, contravened the provision of Article 2.5 of the NDPR and thereby interfered with the Applicant's right to privacy as guaranteed under Section 37 of the Constitution; the Respondent was restrained from further processing of the Applicant's name and telephone number without a lawful basis; and the Respondent was directed to pay the sum of NGN 5 million (approx. $3,358) as damages to the Applicant.

The scope of the NDPR 2019 was strictly on personal rights of Nigerian citizens as guaranteed under the Nigerian 1999 Constitution (as amended). In fact the latter case of *Incorporated Trustees of Ikigai Innovation Institute v. National Information Technology Development Agency (NITDA)*[15]affirms the limited scope of the NDPR when it struck down the Whitelist issued by NITDA under the NDPR Implementing Framework. The Court held that the inclusion of countries without adequate data protection laws or independent supervisory authorities in the Whitelist violated in Article 2.11 of the NDPR.

Furthermore, the Court expatiated that the inclusion of Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) into the NDPR Implementing Framework had no corresponding legal basis or provision under the NDPR. The implication is that the NDPR strictly protected private data of Nigeria living in Nigeria or outside without any reference to cross-border business activities. This exposes the NDPR 2019 severe gaps in regulating data-aligned or digital businesses in Nigeria and outside and the revenue loss to Nigeria is severe. This weakness shows that the NDPR 2019 was not e-commerce or digital trade-oriented.

2.2.Digital Trade under the Nigeria Data Protection Act 2023

The Nigerian Data Protection Regulation 2019 was the first legal framework governing data

[15] FHC/ABJ/CS/1246/2022 (Unreported)

governance in Nigeria under the regulatory power of the National Information Technology Development Agency (NITDA) regarding issues of regulate cross-border data transfer among others. Presently, the National Data Protection Act (NDPA) 2023 is the flagship legislation integrating the NDPR as procedural as subsidiary instrument to set procedural mechanism for efficient implementation of the NDPA 2023 until the issuance of the General Application and Implementation Directive 2025[16]. At the threshold of conflict, the NDPA 2023 prevailed as the principal law[17]. Prior to the enactment of the NDPA 2023, there was the Nigerian Data Protection Regulation Implementation Framework (NDPIF); and one of its objective was the classification of cross-border data transfer procedures.

The NDPF provided for Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR) as alternative data transfer windows without a corresponding in the NDPR, which awash its implementation with ambiguity and superficiality. The pre-NDPA case of *Incorporated Trustees of Ikigai Innovation Initiative v. National Information Technology Development Agency (NITDA)*[18] *affirms the limited scope of the NDPR where* brought its validity to the searchlight of the court where the court decided that inclusion of SCCs and BCRs under Art. 2.11 of the NDPF was a serious violation of the NDPR 2019. The ambiguous whitelist was therefore struck down by the court.

The Nigeria Data Protection Act 2023 is currently the flagship legislation regulating data governance within the Nigeria's sovereignty as it affects relationship with other national, supra-national and multinational entities[19]. The Act generally prohibits cross-border data transfer from Nigeria except under two conditions that—data transfer from Nigeria can only flow to third nation or international corporations with adequate protection and the data subjects derogate. Derogation explains data subject consent or overriding public interest. The two exceptions were transplanted from the General Data Protection Rules (GDPR) 2018).[20]

---

[16] General Application and Implementation Directive 2025, art. 3(3)

[17] National Data Protection Act (NDPA) 2023 s 64

[18] Incorporated Trustees of Ikigai Innovation Initiative v. National Information Technology Development Agency [2023] Unreported FHC/ABJ/CS/1246/2022

[19] STEPHANIE and IYANUOLUWA et al. Reforming Data Governance in Nigeria: A Critical Analysis of the Nigeria Data Protection Act, Regulatory Enforcement, and Global Alignment. *International Journal of Law Management & Humanities,* Vol.7, n6, 2024, pp. 2481 – 2495. DOI: 10.10000/IJLMH.119827

[20] Diana Uzor and Bukola Adesokan, 'Operationalising the NDPA: Bridging Digital Boundaries with Cross-Border Data Rules' (Tech Hive Advisory Africa, 11 September 2023) https://www.techhiveadvisory.africa/insights/operationalising-the-ndpa-bridging-digital-boundaries-with-cross-border-data-rules accessed 28 September 2024

The NDPA 2023 does not generally provide for 'digital trade' in its Definition Section. However, it regulates the important component of digital trade which is data flows and data-aligned business activities such fintech, cloud services, digital banking activities, cross-border services which depend on data processing and transfer for digital trade policy analyses. This implies that data governance in Nigeria remains the fulcrum of digital economy in alignment with the Data Protection Act stating one of the central objective of the Act which is to,

> strengthen the legal foundations of the nation's digital economy and guarantee Nigeria participation in regional and global economies through beneficial and trusted use of personal data[21].

The cited provision elicits the main characteristics of multilateralism which is Nigeria's digital trade '*participation'* among many jurisdictions which are '*regional and global economies'*. The Nigeria Data Protection Act, 2023 (NDPA) is the main regulatory architecture regulating digital trade in Nigeria. It sets guidance for processing personal information for facilitating Nigeria's *participation in the regional and global digital economy*[22].

The NDPA 2023 further regulates digital consumer protection governance. It enforces users' rights to access, amend, and requests the removal of personal information as a boost for local and international consumer confidence in Nigerian digital trade[23]. It regulates digital businesses in Nigeria through valid registration and legal oversight over their operation by the Nigerian Data Protection Commission (NDPC). Tech firms and various digital platforms must validate their legitimate business activities, contractual requirements and mandatory user consent to seamlessly operate in Nigeria. The NDPA establishes the Nigeria Data Protection Commission (NDPC) to perform oversight responsibility on digital corporates with respect to incorporation and periodic check on the lines and procedures of operations of the tech entities to ascertain their global competitive market drives while avoiding breach of Nigerians privacy rights[24].

[21] National Data Protection Act 2023, s. 1 (h)
[22] Section 1 (h) of the Nigeria Data Protection Act 2023
[23] EKPETE AND EKPETE. Legal and Economic Perspectives of the Data Protection Act in Nigeria. Nnamdi Azikwe University Journal of Commercial and Property Law, Vol. 13, n2, 2026.
[24] BOLARINWA L. and OSADOLA I. 2022. Issues with Enforcement of Religious and Allied Obligations under the New CAMA, Usman Dan Fodio University Journal of Private and Business Vol. 2 No. 3 pp. 80-91 ; Part VI of the NDPA 2023

2.3. General Application and Implementation Directive (GAID) 2025

The Nigeria Data Protection Commission (NDPC) released the General Application and Implementation Directive (GAID) as an operational or implementation guideline for the Nigeria Data Protection Act[25]. The GAID replaced the defunct National Data Protection Regulations (NDPR) 2019 to position data governance for efficient delivery[26]. The GAID sets a practical framework for data-related digital trade, particularly as it relates to cross-border data flows, consumer consent, and the deployment of emerging technologies, including fintechs, cloud services, and regtechs, among others.

The GAID is a bridging building framework between domestic and international digital trade activities regulating data-aligned digital trade key instruments including cross border data flows, emerging trade technologies to conduct digital businesses where data information is of essence[27]. The GAID provides that technological firms in Nigeria can only supply or transfer business data if the receiving/user countries have functional *adequate* privacy protection framework, digitally-aligned Standard Contractual Clauses (SCCs) and adaptable Binding Corporate Rules (BCRs) to fulfil the legal/regulatory requirements to open Nigeria's digital trade to global opportunities and benefits.

Furthermore, regarding emerging trade technologies including fintechs, regtechs, freight platforms, AI platforms, crypto/blockchain digital markets, GAID strictly enforces compliance of these digital markets to the requirement of Data Privacy Impact Assessments (DPIAs), legal procedures of anonymized consumer data, and periodic oversight on algorithms to avoid breach of privacy rights and unhealthy business outcomes[28]. The GAID also directs digital corporates to create their user interfaces and data documentation procedures to guarantee safety of the unprotected populations from predatory data gathering. This is referred to as vulnerability index assessment to enhance equitable benefits of various geo-demographic actors including digital corporations, the low digital literates, and vulnerable data users[29]. The GAID has subtly harmonized data processors components for operational efficiencies to promote ease of doing

---

[25] NDPC/NDP ACT-GAID/01/2025

[26] G. Elias & Co. Highlights of the Nigeria Data Protection Act General Application and Implementation Directive, 2025. https://www.gelias.com/images/Highlights_of_The_GAID.pdf

[27] GAID, art. 26

[28] GAID, art. 44

[29] GAID, art. 6 (2)

digital businesses among others.

2.4. Analyses of Digital Trade Protectionism under the Nigerian Legal Framework

Historically, Nigeria data governance operated under the Nigerian Data Protection Regulation (NDPR) 2019 before transiting to a full parliamentary enactment of data legislation and governance in 2023. The Nigeria Data Protection Act (NDPA) and General Application and Implementation Directive (GAID) regulate data governance in the domestic and international digital businesses affecting the Nigerian sovereignty. The NDPA as flagship legislation regulates cross-border data transfer and localization of data which are core components and determine the nature/strategy of digital trade adopted by Nigerian sovereignty. Nigeria included the two components in its data laws implement them under strict and extreme conditions. Similarly, the GAID sets out implementation procedures for the legislation to strictly enforce its economic philosophy of digital trade protectionism. This paper critically analyses the provisions of the three legal frameworks and their economic effect within the global business space.

a. Digital Protectionism under the NDPA 2023

Every jurisdiction is under sovereign responsibility to protect both its businesses and rights derived therefrom for its citizenry. However, protectionist measures should not hamper regional and international business benefits. The Nigeria Data Protection Act 2023 regulates cross-border data transfer and localization of data as it relates to both domestic and international digital trade[30]. The NDPA 2023 does not directly regulate digital trade but data flow and it is structured as a protectionist measure to limit or restrict cross-border data transfers and enforce localization of data businesses to protect domestic businesses and strictly favour personal data rights against foreign competitors[31].

The operational statement of section 41(1) of NDPA states,

> A data controller or processor shall not transfer personal data outside Nigeria…

[30] NDPA 2023, ss. 41-43
[31] BOLARINWA LEVI. 2022. Issues with Piracy Regulation in the Nigeria’s Waterways, Benue State University Law Journal (BSULJ) Vol. 10, Number 1 pp 32-41

This statutory provision cited carries mandatory structure of prohibiting data transfer from Nigeria's territory to another jurisdiction. This generally festers digital trade protectionist tone restricting data-aligned business information from leaving Nigerian territory. This provision impliedly favours domestic businesses and raises both monetary costs and strict regulatory hurdle for foreign competitors even across African regions, and against the flexible/equitable provision of Article 21 of the AfCFTA Digital Trade Protocol 2024. This provision puts serious burden and bureaucratic bottlenecks. The same section 41 (1) immediately sets out strict conditions for cross-border transfer to take place thus,

> …unless the transfer is made to a country that ensures adequate level of protection, or the transfer is made subject to appropriate safeguards

It can be gleaned from the same section that either one of the two conditions set out must be strictly complied with… *adequacy or safeguard* mechanisms. The Nigerian Data Protection Commission (NDPC) must strictly ensure that the data user/request country must have adequacy measures in place that is substantially related to Nigeria's adequacy standards. This is the condition for such data to be transferred to the user/or request country to avoid case-by-case contracts or Nigerian Data Protection Commission approval before transfer. The combined provision of section 41 (1) of the NDPA and Regulation 45 of the GAID place unlimited power on the NDPC to declare a country adequate or not.

A country's adequacy condition is measured on the following components which must be *simultaneous and mutually inclusive*—rule of law and privacy rights, protection mechanisms, enforcement/redress against breach, international data obligations, and further transfer mechanism[32]. A user/request country must practice rule of law and human rights that enforce data privacy protection, functional data protection law and administrative and judicial remedies against subject data breaches. For instance, the NDPC must get assurance that the Nigerian data subject can seek redress abroad against the violation of his personal data rights[33]. The user/request country shall be a member of data-aligned international OECD Convention to invoke Art. 48 of which no African country is a member. Worst still, invoking the AfCFTA Digital Trade Protocol 2024 is of no consequence outside Africa. The only respite is that the

[32] NDPA, s. 42(4)
[33] BOLARINWA LEVI AND JEMILOHUN BERNARD. 2021. Issues with Comprehensive Database Regime in Nigeria: Any Way Out? Ife Juris Law Review (IFJR) Vol.2, pp. 80-87 NDPA, s. 40(3)

user/request country must have legal framework that allows it to only transfer the same data to third country with adequate protection.

However, Nigeria does not currently have adequacy template to enforce the simultaneous conditions analysed above. Since the enactment of NDPA in 2023 and operation of data governance, Nigeria has not granted or issued adequacy status to any country. This implies that many advanced commercially viable digital trade regions and nations including the EU, UK, Kenya, Ghana, do not qualify to trade with Nigeria particularly as the commerce involve data transfers[34]. The user/request countries that set to engage in digital trade arrangement can only invoke the *safeguard mechanism* structured into Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs) and other NDPC pre-approval measures. In fact, the GAID provides that the NDPC approval is pre-conditional to harnessing the alternatives route SCCs/BCRs and the contract must be submitted with the Transfer Impact Assessment[35].

Further, section 41 (4) of the NDPA enforces data localization in the Nigeria territory alone. The Nigerian Data Protection Commission (NDPC) categorizes some data as sensitive and classifies them under localization status. This implies that such sensitive data are regulated under stricter rules. Nigeria has yet to issue Localization List and Template, but some sensitive institutions of Nigeria Government including the Central Bank of Nigeria has issued rules directing all Biometric Verification Number (BVN) data to stay[36]. Prior to its defunct status in 2025, the NITDA rules restricted sovereign data transfers. The GAID also regulates using Data Protection Impact Assessments (DPIAs) and Transfer Impact Assessments (TIAs) to restrict data transfer outside Nigeria[37]. The danger therefrom reflects that even if the NDPC approves data transfer, the sector-specific transfer may still be restricted by CBN, NITDA among others until they give their approval.

b. Digital Trade Protectionism under GAID 2025

The General Application and Implementation Directive (GAID) 2025 is an operational guideline for the NDPA 2023 in digital data governance. The GAID 2025 is a policy direction

[34] Under the Nigeria Data Protection Act (NDPA) and its operational GAID, countries are generally disqualified from data transfers, except under certain contractual arrangements, SCCs and BCRs to allow data flows.
[35] GAID, art. 45
[36]EHI. A Critical Analysis of the Bank Verification Number Project introduced by the Central Bank of Nigeria. *SSRN Electronic Journal* Vol. 2, n3. 2015. DOI: 10.2139/ssrn.2544934
[37] G. Elias & Co Newsletter, pg.4

that sets out mechanisms for enforcing protectionist measures in digital trade[38]. The GAID strictly enforces cross-border data flows and data localization regime as allowed under the NDPA 2023 and the effects of its implementation is digital trade protectionism[39]. The salient components of the Directive that promotes digital business protectionisms are analyzed.

The first protectionist measure of the Directive is pre-approval requirement for data transfers by the Nigerian Data Protection Commission. Article 45 which is the implementation provision of section 41 (1) of the NDPA 2023 mandates the NDPC to approve all Standard Contractual Clauses (SCCs) and Binding Contractual Rules (BCRs) before data can be transferred outside Nigeria to the requesting/user countries. The bureaucracy of validating or rejecting the data by the NDPC can significantly delay the urgency of the business-aligned data requests. The processing costs expended, time of waiting, delay impact on the digital businesses, unregulated corrupt practices of the NDPC officers and in case of eventual rejection, create legal uncertainty and strict protectionism, which is not viable for flexibly or equitable global digital trade standards. The GAID does not set timeline for NDPC approval of the requested data which can even exceed the time value for transfers of the data if eventually granted[40].

The second protectionist measure by the Directive is under Article 45 (3) compelling transfer impact assessments (TIAs) for every cross-border data requirement. The TIAs must state clearly that the requesting/user country has similar adequacy status with Nigeria, whereas Nigeria has not published its Adequacy List, hence the SCCs and BCRs alternatives which are more uncertain, rigorous and forlorn[41]. The rigor on the Nigerian corporate entities requesting for approval from the NDPC makes the TIAs approval unrealistic than certain. This aligns with the decision of Obiora Atuegwu Egwuatu, Judge of the Nigerian Federal High Court in *Kigai v.NITDA* thus,

> I have critically examined the provisions of Articles 2.11 and 2.12 of the NDPR and it is correct that the two new mechanisms

[38] GAID, art. 3 (1)

[39]BOLARINWA LEVI. 2021. Non-special Criminal Forum for Securities Case: Remedying Investors' Confidence in the Market, University of Benin Journal of Business Law (UBJBL) Vol. 1 Number 1, pp. 113-125 file:///C:/Users/user/Downloads/BALANCINGDATALOCALISATIONANDREGIONAL-INTERNATIONALTRADE.pdf

[40]The GAID foists critical bottlenecks and lacks specific statutory timeframe or Service Level Agreements (SLAs) for NDPC application processing, having consequential and protracted delays that defeat the real-time business value of the data.

[41] In *Kigai v. NITDA*: The court held that the countries on the Whitelist without a data protection law and/or a data protection authority are inappropriate, and the list should be reviewed to comply with the law.

were not so provided for in the NDPR nor was any procedure or steps to comply with the said mechanisms[42].

The protectionist requirement of five-fold adequacy status components from user/requesting country which include rule of law and privacy rights, protection mechanisms, enforcement/redress against breach, international data obligations, and further transfer mechanism, constitute serious barrier to ease of doing digital businesses with Nigeria[43]. In fact, small or SMEs digital businesses in Nigeria and foreign countries can take the resource-intensive legal and bureaucratic risks of assessment requirements. There is no *de minimis* provision in the legal framework to classify cost layers for digital firms according to their sizes, the processing costs and administrative rigours are the same with large digital business entities with high stake of uncertainty[44].

The third protectionist measure is captured under the GAID which makes localization status stricter and enforces sector-specific localization rules[45]. For instance, the digital financial entities under the Central Bank of Nigeria must reside their data-specific information in Nigeria[46]. The Biometric Verification Number (BVN) personal data in Nigeria, sovereign data under their trust must not leave Nigerian shore unless approved by both the NDPC, which is more unrealistic, rigorous and stricter[47]. The framework protectionist measure has limited foreign fintech entities, regtech entities, healthtech entities and cloud services to consult domestic partners in Nigeria to provide their needed digital trade services[48]. The Nigerian start

[42] At p.19, Para. 2 of the judgment

[43] MASSIMO. Transferring personal data to international organizations under the GDPR: an analysis of the transfer mechanisms. 2023. *International Data Privacy Law*, Vol. 14, n 1, 2023. pp. 1-18 DOI: 10.1093/idpl/ipad022

[44] The gap in progressive *de minimis* thresholds or scalable compliance tiers brings a dangerous regulatory trap for small digital businesses. Startup firms and budding entities are compelled to absorb disproportionate fixed costs and administrative burdens, which serves as innovation barriers and indiscriminately favor multinational corporates.

[45] GAID, art. 48

[46] UBANI and ADEYEMI. REGULATION OF DIGITAL BANKING IN NIGERIA. *Castle Law Journal (CLJ)* Vol. 2, n. 1, 2023, p. 101; BOLARINWA L.P. & OGUNFOLU A.O. (2020). Exigency for Commercial Court Establishment for Ease of Enforcement of Contract in Nigeria; UNILAG Law Review (Print) Vol.4, n 1

[47] CBN Publication. Addendum to the Revised Regulatory Framework for Bank Verification Number Operations and Watch-List for the Nigerian Banking Industry. (*Circular PSP/DIR/PUB/CIR/001/002, March 2026*) https://nibss-plc.com.ng/wp-content/uploads/2026/04/BVN-Circular.pdf; Bolarinwa L.P. & Abifarin F. (2019). Issues with Arbitral Resolution of Securities Disputes in Nigeria: Any Viable Reform? Federal Ministry of Justice Journal (FMJJ) Vol.5 pp. 178-202

[48] OLUWASOLA and ABAYOMI et al. Regulating fintech for financial stability in Nigeria: balancing cybersecurity risks and financial inclusion. *African Journal of Economics and Business Research*, Vol. 4 n 2, 2025, pp. 84-85. DOI: 10.4314/ajebr.v4i2; BOLARINWA LEVI. (2020). Issues with Asset Declaration by Ban Employees in Nigeria: Any Exigency for Reform? Federal University Oye-Ekiti Law Journal (FUOYELJ) Vol. 2, 2020, pp.106-114

–up digital entities continue to struggle under the protectionist governance while the foreign digital businesses in Nigeria has options of exiting and migrating to other jurisdictions with flexible data-aligned digital governance.

c. Digital Trade Protectionism in Nigeria under the AfCFTA Protocol on Digital Trade 2024

Nigeria is a frontline member of the AU and the African Continental Trade Agreement (AfCFTA). Nigeria was the first country to sign and ratify the AfCFTA Protocol on Digital Trade 2024[49]. The Protocol drives a default *anti-protectionism governance* among the regional members, allowing flexible and equitable cross border transfers among signatory members[50]. It is a default Protocol because it defers to member states reasonable public policy protection of domestic interests. The Protocol enforces free data flows, voiding domestic localization restrictions[51]. This aligns with the exact provision of Art. 20 of the Protocol that, "Each Parties shall allow cross-border data flows for the conduct of digital trade..," This cited provision aligns with Art. 21 to drive *anti-protectionism governance* that,

> Parties shall not require a firm to use or locate computing facilities in their territory as condition for doing business

The cited provisions generally imply that protectionist measures are prohibited, except under reasonable condition for public policy interest and proportionality principle and such default condition must be open, transparent and reasonably convincing[52]. Even though section 41 (4) of the NDPA 2023 gives exception for waiving localization status, the exceptions are stricter, forlorn, with legal uncertainty and bureaucratic bottleneck. The section also defers to sector-specific localization rules such as the Central Bank of Nigeria (CBN) rules which strictly compel data-aligned digital banking to situate Biometric Verification Number (BVN) in the Nigerian territory and NITDA Rule also strictly compel that sovereign data/digital information

[49] SUCKER. (2026). "The AfCFTA Digital Trade Protocol", in Birhanu, F. M., Hailu, M. B., Klimke, R. & Tietje, C. (Eds.), Handbook on the African Free Trade Area *Routledge*, 2026; BOLARINWA L.P. (2023). Enforcement of SDG 3 –Good Health and Well-being- in Nigeria, Nigerian National Human Rights Commission Journal (NNHRCJ) Vol. 9 & 10 pp.67-90;

[50] AfCFTA Protocol on Digital Trade (PDT) 2024, art. 7; BOLARINWA L.P. and OKORODUDU-FUBARA M. (2020). Capturing All Financial Services under a Specialized Court for Investment Growth in Nigeria, UNILAG Law Review (Print) Vol.4 Edition 2

[51] AfCFTA PDT, art. 7(2)

[52] AfCFTA PDT, art. 8

must not leave the Nigerian shore[53].

It is suffice that sector-specific localization has been flexibly addressed under the Protocol referencing public policy interest as exception for transfer refusal[54]. It implies that the Protocol directs the National Data Protection Commission to prove that such non-approval would decimate fraudulent activities of data-aligned digital and cloud services and bring about financial stability and protect anti-money laundry measures[55]. However, the NDPA 2023 does not align with such flexible procedural justification, its provision is pro-protectionist measure of out rightly disapproval or restriction of such transfer without evidence that transparent procedures were followed to allow such disapproval[56]. This friction between the NDPA and AfCFTA Protocol continues to undermine the economic philosophy of regional integration for free trade arrangement. The conflict is so critical because Nigeria is a leading actor in the formation of the African Continental Free Trade Agreement, the first signatory to the AfCFTA Protocol and largest economy in Africa. Non-alignment of Nigeria's digital trade protectionism with anti-protectionism of the protocol particularly in e-commerce regime will continue to clog the objectives and opportunities inherent in the AfCFTA agreement[57].

Nigerian digital trade protectionism under section 41 (1) of the NDPA 2023 and similar provision of the GAID 2025 are in serious conflict with the anti-protectionism governance provision of Article 20 (1) of the AfCFTA Protocol on Digital Trade 2024. The AfCFTA Protocol freely allows data transfers among the regional members on the default that the member states must show reasonable cause/public policy interests as ground for restraining data within Nigeria. However, Nigeria does not allow data transfer unless such undergo rigid/stricter NDPC adequacy status approval or SCCs/BCRs pre-approval with high-stake of legal uncertainty and bureaucratic fatigue[58]. Nigeria has wrongly transposed the burden of proof under the AfCFTA Protocol by compelling digital businesses to justify why the cross-border data transfer be granted or approved by the NDPC; whereas, the Protocol directs Nigeria

[53] NITDA Guideline 12.1(4); BOLARINWA, L.P. 2018). Inclement Business Regime in Nigeria: Removing Persistent Legal and Bureaucratic Bottlenecks; International Journal of Business and Applied Social Sciences (IJBASS), VOL: 4, ISSUE: 4, pp 12-26

[54] AfCFTA PDT, art. 21 (1)

[55] AfCFTA PDT, arts, 20(2) and 22(2)

[56] NDPA 2023, ss. 41-43

[57] BOLARINWA LEVI. 2020. Tax Regime of Digitized Entities in Nigeria: Issues and Exigency for Reforms; Federal Ministry of Justice Journal (FMJJ) Vol.4 pp. 1-22

[58] Under the Nigeria Data Protection Act (NDPA) and the General Application and Implementation Directive (GAID), cross-border data transfers are strictly regulated and can create serious bottlenecks, even businesses relying on derogation may need to prepare for administrative delays.

to justify why specific transfer must be approved[59]. Nigeria's non-compliance with the default provision of the AfCFTA Protocol on data regulations can continue to undermine digital businesses in the region and restrict digital business investments in the region and the world.

The Annexure of the AfCFTA Protocol aligns with urgency and ease of contract dealing and enforcement by making SCCs and BCRs self-executing and structured into post-transfer auditing to avoid administrative bottlenecks, procedural rigidity and excessive processing costs. The Protocol leverages on accountability than regimented licensing and rigorous bottlenecks of the NDPC approval of the SCCs and BCRs structured in legal uncertainty. The GAID in alignment with the NDPA directs the NDPC, without timeline, to pre-approve cross-border data before any action[60]. This Nigerian protectionist regime creates serious hurdle for intra-AfCFTA trade movement at outrageous costs, administrative bureaucracy, without timeframe, which should have been freely flexible under the regulation of the AfCFTA. Whereas under Art. 20 (2) of the Protocol, the approval measure must be less strenuous and flexible, providing for post-transfer auditing to avoid inclement delay of the business.

3. EU Digital Trade Model and Lessons for Nigeria's Protectionist Governance

The 27-member European Union and European Economic Area (EEA) have a central legal framework regulating their digital trade. The EU General Data Protection Regulation (GDPR) is a flagship governance framework harmonized into the region's Single Market System (SMS)[61]. The EU digital business is integrated within its single market system with a lone objective of aligning data free flow with free movement of goods and services in the region, without compromising privacy standards.

Art. 1 (3) of the GDPR clearly states its central goal of promoting seamless flow of personal data within the EU countries comparatively the same with the AfCFTA Protocol on Digital Trade championing *anti-protectionism* governance. It states that,

> The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the

[59] AfCFTA Protocol, art. 23(1) of the CBDT-Annex.

[60] GAID, art. 45

[61] The EU General Data Protection Regulation (GDPR) is a detailed framework that integrates privacy laws across EU states, serving as a significant foundation for the EU's Digital Single Market. It balances the free movement of data across borders and protection of fundamental consumer rights.

protection of natural persons with regard to the processing of personal data

This preliminary objective provision promote digital trade in a way to avoid deploying data protection as a disguise to create trade barriers across the region and beyond. The provision interprets privacy as a fundamental right but not as a clog to stalemate or fragment liberalization of digital market[62]. The logic is to reinforce the philosophy of single market framework to liberalize free movement of goods and services which thrive on data. However, Nigeria's NDPA 2023 and GAID 2025 drive digital trade protectionism strictly hoarding its business-aligned data from competing flexibly across the African region of which it is a frontline member of African Union and a signatory to the anti-protectionist AfCFTA Protocol on Digital Trade 2024 and also limiting its e-commerce trade at the global space[63].

Nigeria can glean and learn from Art. 1 (3) of the GDPR which is significantly dubbed as an anti-protectionism clause allowing free data movement across EU member states and within the EEA without compromising personal rights defence under Art. 1 (1) and (2) which must be transparently justified before the EU Commission. Nigeria may need to review its data laws in alignment with the constitutional clause/core of Art. 1 (3) of the GDPR. This is plausible in Nigeria by transplanting and modelling anti-protectionist clause into the NDPA and in conformity with the material objective of the AfCFTA Protocol on Digital Trade 2024 to promote regional single market[64].

The top-tiered Scope provision of section 1 of the NDPA and Art 1 of the GAID may need to be amended softly and flexibly without compromising privacy rights as the case of the EU GDPR and TFEU provisions. Nigeria just needs to flexibly set a default clause by generally removing severe restriction or prohibition clause banning data movement to AfCFTA member states that are signatories to Protocol on Digital Trade 2024.

National, health or public safety cannot be a blanket reason for sovereign authority retaining business-aligned data in Nigeria, proof of such retention must overwhelmingly serve public policy interest why data transfer must be restricted from flowing to AfCFTA member states,

---

[62] GDPR, art.8
[63] The rigid provisions and interpretations of sections 41-49 of the NDPA 2023conflicts with the flexible interpretation of the EU GDPR in balancing privacy rights with free-flow of data-aligned businesses across the EU-member states and beyond.
[64] AfCFTA PDT, arts. 20-22

third countries or international corporations. This was the decision of the ECJ in the landmark case of *La Quadrature du Net*[65] on matter relating to digital privacy, data retention and online copyright regulation that indiscriminate mass data collection severely infringed on the fundamental rights of EU citizens under the *e*Privacy Directive and the EU Charter on Fundamental Rights. The Court said that national security breach is severe in nature, and required seizure and retention of such crime-specific data, but not general data. However, ECJ said such data retention or seizure of specific subject of crime, must be by court sanction[66]. Nigeria can model its framework after the ECJ's decision of differentiating general data retention from crime-specific date retention, and retain only crime-specific data, while allowing business-aligned data movement within and outside the region.

Art. 44 of the GDPR sets out general principle for cross-border data transfer across the European Union and European Economic Area and to third countries transfer of data. It states that intra-region cross border data transfer is free and seamless while transfer from the EU/EEA to third countries outside the EU/EEA shall be enabled only if all the conditions set out for such transfer in the Regulations are met[67]. The transfer conditions are clearly set out in their categories from the succeeding Articles. Art. 44 is anti-protectionist general scope applicable to third countries and be invoked any time data is transferred to third countries regardless of whether the processor is within EU/EEA territory while the servers are outside the territory. This implies that an EU-member state cannot resist or restrict data transfer to other intra-EU states nor restrict transfer to third-country businesses, neutralizing classic protectionist measure of using private rights as a disguise to shut out offshore business services.

In *Maximillian Schrems v Data Protection Commissioner*[68]*,* the ECJ struck down in its entirety the Data Protection Commission (DPC)'s decision 2000/520/EC. The reason was that US law obliged state regulators to generally access data transferred under Safe Harbour, beyond what is essentially and strictly equivalent under the EU data protection requirements. The ECJ observed that US data laws allowed the regulatory authorities to have general access to data

---

[65] Case C-511/18—La Quadrature du Net and Others v. Premier Minisre and Others, ECLI:EU:C2020:791[2020]

[66] The European Court of Justice (ECJ/CJEU)) has repeatedly decided that the issue relating to privacy rights and data protection must undergo strict judicial oversight in line with the EU Charter

[67]VOLOSEVICI, Transfers of Personal Data to Third Countries or International Organisations. An Overview of the European Legal Regime. *Journal of Law and Administrative Sciences*, n 12, 2019*,* pp.73-74. file:///C:/Users/user/Downloads/TRANSFERSOFPERSONALDATATOTHIRDCOUNTRIESORINTERNATIONALORGANISATIONS.ANOVERVIEWOFTHEEUROPEANLEGALREGIME.pdf

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

transferred by the Safe Harbour which breached the EU privacy rights laws on retention . The ECJ agreed that the US has to safeguard national security and public interest like EU laws which also safeguard national, health and privacy security, but must not be general, mass or traffic data retention or access[69]. This is a serious conflict between the US and EU requirements. The ECJ ruled that such general access and transfer to the US under Safe Harbour constituted unlawfulness, it should have been limited to specific data that related to the US public interest breach.

It is a significant lesson for Nigeria to publish its own adequacy list modelled after the EU and ensure that does not distort data-aligned businesses with third countries or international corporates as enumerated in the *Maximillian case*. This may need to begin with amendment of the umbrella section of the NDPA 2023 by allowing public authorities to retain, access only crime-specific data and not general or traffic data which may destroy foreign businesses involving third countries or international corporations as decided in the *Schrems case*. Similarly, Nigeria may need to establish regional flexibility of data flow in accordance with the AfCFTA Protocol on Digital Trade.

The legal transplant of Art. 44 of GDPR into the Nigerian data framework will then allow data transfer from Nigeria to AfCFTA member states that are signatories and have ratified Protocol on Digital trade including prospective member states, without setting conditions for adequacy status, Binding Contractual Rules or Standards Contractual Clauses. This is grounded on the philosophy that African Free Continental Trade Agreement (AfCFTA) was comprehensively agreed to foster free movement of trade among the member states, preparing space for single market system. Liberal market structure should not be a matter of policy paper alone, Nigeria as a frontline actor in African Union mandate, should practically through common legal framework help the regional trade exchanges thrive on flexible anti-protectionist governance.

Art. 45 of the GDPR states one of the conditions for third country or international organization or corporations in the third country which is *adequacy status.* Art. 45 (1) states that,

> A transfer of personal data to a third country or an international organization may take place where the Commission has decided

[69] EU GDPR, art. 23

> that the third country, a territory or one or more specified sectors within that third country or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization.

The provision above neutralizes administrative bottlenecks, avoid regulatory burdens and erase financial extortions in getting authorization from the EU Commission. The verification and justification of *adequacy status* of third countries is self-executing and "*shall not require any specific authorization*." This provision aligns with tone of commerce and multilateralism proportionate to timeframe and comparative legal and administrative advantages. The mechanism is that the Commission just needs to grant adequacy status to countries on the strength of their meeting the requirement. Once given, there is no duplication of authorization, the third countries enjoy the same data transfer like the domestic or EU-member states. Art. 41 (2) highlights elements/components that constitute *adequacy status*.

Nigeria can also replicate the EU GDPR data transfer regime to third countries or international corporations where those corporate entities can harness Standard Contractual Clauses (SCCs), Binding Contractual Rules (BCRs) without getting pre-approval from the NDPC. Nigeria just needs to urgently issue/publish its adequacy list and grants adequacy status to third/foreign countries or international corporations that align with personal data adequacy requirements and the conducted can be dematerialized. The NDPC, upon request, just need to conduct Transfer Impact Assessment, append *e*-signature on it where there is no presumption of irregularity or fraudulent practice, and then transfer[70].

Nigeria needs to discard the provision for pre-approval license which constitutes administrative bottleneck, excessive cost implication and festers classic protectionism and complicate ease of doing and enforcing digital businesses. In fact, data transfer to third/foreign countries or international corporations should align with Art. 45 (1) which is self-executing and "*shall not require specific pre-approval authorization*"

Art. 46 highlights the safeguards for such data transfers which include binding and enforceable instruments between regulatory authorities or bodies. These safeguards are: Standards Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). The provision places

[70]EU GDPR, art. 45 (1)

significant task or burden on the regulators to prove or justify why data must not be transferred or migrated outside the shore of the EU, while the offshore digital corporates need not get permission or authorization for access. This is to guarantee transparency, accountability and equitable trade treatments across the world. Art. 46 of the GDPR is reinforced under Art. 52 (1) of the Treaty on the Functioning of the European Union (TFEU) which flavoured the EU anti-protectionism governance against any nationally-designed protectionist rules. The provision safeguards the interest of foreign nationals or entities under the principle of fair treatment thus,

> The provisions of this Chapter and measures taken in pursuance thereof shall not prejudice the applicability of provisions laid down by law, regulation or administrative action providing for special treatment for foreign nationals on grounds of public policy, public security or public health.

The combined provisions of Art. 46 of the GDPR and Art. 52 (1) of the TFEU set out *special treatment for foreign nations*… which include foreign entities or corporations to the effect that significant burden of proof is placed on the EU Commission or any EU member state to establish that restriction on data transfer is non-discriminatory, proved by public policy and proportionate. This governance aligns with the ECJ decision in *Maximillian Schrems case* where it was decided that however valid the Standard Contractual Clauses (SCCs) or Binding Contractual Rules (BCRs), there must be evidence that the third country guarantees "*essentially equivalent*" protection.

The Court held that the US surveillance laws: FISA 702, EO 12333, did not accord proportionate legal redress for EU citizens whose rights were violated and therefore, declare indiscriminate and disproportionate under Arts. 7, 8, 47 of the EU Charter. Nigeria needs this innovation in its NDPA 2023 and GAID 2025 to proportionately balance privacy rights and business rights particularly when relating with the third countries or businesses to promote *essential equivalence* between Nigeria and Europe and other third countries and international corporates.

Art. 6 of the GDPR loudly supports principle of proportionality, non-discrimination and fair treatment in data transfer governance. The European case law of *European Commission v.*

Republic of Austria[71] strengthens this anti-protectionist measure when the Court ruled that Austrian authority could not restrict all health data to stay in Austria, and the Austrian law was discriminatory, disproportionate, and violated public policy governance and contravened the combined provisions of the GDPR and TFEU.

Art. 46 of the EU GDPR protects foreign digital businesses without compromising sovereign data governance and regional digital businesses. Nigeria can glean a lesson from the provision by creating conducive data-aligned businesses free from hostility, discrimination. Corporate firms find clement regulatory environment to thrive their businesses, while Nigeria can replicate favourable business treatment of foreign digital entities by strengthening its oversight function over digital corporates within and outside its shore and fairly aligning its law with EU standards of anti-protectionism governance.

Art. 60 of the GDPR regionalized enforcement against fragmented or conflicting national laws of EU member states, restricting EU-member states from unilaterally blocking or banning data transfer. The provision establishes one-stop administrative structure issuing common policies binding and enforceable across EU and EEA states and by regulatory concession, foreign nationals or corporate entities. For instance, if Germany allows a transfer procedure, Spain cannot restrain or restrict its implementation under its national law, as such action will breach binding single market principle pursuant to Art. 56 of the TFEU and similar anti-protectionist regional laws.

The EU has harmonized all the regional trade laws including data-aligned digital trade laws into a comprehensive regional legislation to avoid conflict in driving single market system. Art. 60 of the EU GDPR is anti-fragmentation clause enforceable against fragmentation of the EU Single Market System. Art. 22 of the AfCFTA Protocol on Digital Trade advocates for 'economic integration' without a complementing operational clause like Art. 60 of GDPR to foster common or single market for Africa. Hence, Nigeria, as a strong member and signatory to AfCFTA Protocol on Digital Trade can muster political and diplomatic will to lead other member states to replicate Art. 60 of the GDPR into the Protocol. However, Nigeria has to reform itself before replicating the obligations at the regional level.

Therefore, Nigeria can replicate the provision of Art. 60 to integrate or harmonized its

[71] Case C-614/*10 European Commission v Republic of Austria* ECLI: EU: C:2012:631. [2012]

conflicting data protection law. For instance, all matters relating to data utility-collection, processing and transfer should be harmonized into one-stop legislation as the case of the EU. Hence, the sector specific laws such as the Central Bank of Nigeria's stricter/protectionist regulation of Biometric Verification Number (BVN) data among others need to be harvested into one stop regulatory framework to avoid conflict of policy implementation and fragmented administrative hurdle.

Furthermore, to avoid overregulation and conflicting policy administration of data system in Nigeria, the Nigerian Data Protection Commission (NDPC), Central Bank of Nigeria, NITDA, Nigerian Bureau of Statistics (NBS) must align their regulatory responsibilities on their sector specific administration into one-stop shop mechanism to sustainably promote ease of doing and enforcing data businesses in Nigeria

Localization status does not have a foundation in the GDPR and similar EU regional laws. It is not practicable or enforceable as a rule under Single Market Rules. This classic protectionist measure directing foreign corporates to situate a partners among local companies or relocate their digital trade assets to any EU member state is not adopted or ratified. The EU GDPR has no provision for digital border but technology-driven data flow governance. The EU legal norm is structured with a pathway of strengthening *e*-governance and *e*-regulation against physical supervision and bureaucratic fatigue of physical procedures. Dynamic remote sensing coordination procedures structured into enforceable paperless agreement would achieve the same goal better and faster than regimented or protectionist *localization status*.

The decision of the European Court of Justice (ECJ) in *Digital Rights Ireland Ltd v. Minister for Communication*[72] is apt in condemning indiscriminate or disproportionate EU General Data Retention Directive. The ECJ rejected mass/traffic data retention as a serious violation of privacy rights. The Court ruled that for a retention or access to be justified on the ground of specific and differentiated retention, the sovereign authority must justify its action under overridden public security and safety. Localizing/retaining general, traffic or mass data by EU member state is violates Arts. 7 and 8 of the EU Charter.

Nigeria may need to expunge localization status from its data law to replicate the extant provision of the EU GDPR and in alignment with ECJ's *Digital Rights Ireland case*,

[72] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland v Minister for Communication, Marine and Natural Resources and Others, (ECLI:EU:C:2014:238)

prohibiting localization or seizure of traffic or mass data without specifically linking them to threat to national or public safety. The EU Court applied the principle in the case of *Tele2 Sverige & Watson*[73] that sovereign laws cannot compel indiscriminate and general retention of mass/traffic data without judicial sanction under case-by-case evaluation of facts. Nigeria can amend its NITDA rules mandating localization of general data by national/regulatory authority such as CBN unfair retention of Biometric Verification Number (BVN) data in Nigeria without timeframe. The laws can be amended to mandate court sanction of such retention, upon case-by-case proof for such retention, compelling regulatory authorities to establish case-by-case proof to justify the retention. As an emerging digital economy, the CBN with other data-aligned business regulators needs to review its protectionist governance by replicating the EU borderless digital governance of technology-driven regulatory platform for **e**-regulation and *e*-governance.

4. Conclusion

Nigeria is emerging gradually as Africa's digital trade hub and enacting its legal frameworks to regulate it. However, its digital trade law particularly business-aligned data laws including Data Protection Act 2023 and GAID 2025 are protectionist in nature and makes it difficult for digital trade including start-up technology entities, fintechs to expand within Africa; and strenuous for the Nigeria-EU digital trade exchanges and other third countries and corporations to consider Nigeria as a viable business climes. This paper has comparatively shown how the EU model harmonized its data laws and utilities to expand its Single Market System. . It observed that Nigeria data laws conflict with the anti-protectionist measures of the AfCFTA Protocol on Digital Trade which needs urgent alignment to fully balance regional enforcement of privacy rights with flexible digital trade expansion. The paper has shown how Nigeria can replicate the EU model without choosing between privacy and trade, but integrate both under a comprehensive data law that is proportionate, non-discriminating and equitable.

[73] Joined Cases C-203/15 AND c-695/15 Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December (ECLI: EU: C: 2016: 970)