

**CROSS-BORDER DATA FLOWS AND DIGITAL TRADE
INTEGRATION IN AFRICA: LEGAL INTEROPERABILITY AND
DOMESTIC ALIGNMENT UNDER THE AfCFTA**

by

Abdullahi M Abdulquadir

**A thesis submitted to the Graduate Program in Law in conformity with the requirements
for the degree of Master of Laws**

Queen's University

Kingston, Ontario, Canada

February, 2026

Copyright © Abdullahi M Abdulquadir, 2026

Abstract

The governance of cross-border data flows has become a key legal issue for digital trade integration in Africa. This is evident in the adoption of the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol and its Annex on Cross-Border Data Transfers. This thesis examines how the governance framework for cross-border data flow under the Protocol and its annex interact with domestic cross-border data flow governance. Using a comparative legal approach, the thesis studies Nigeria, Kenya, and South Africa as examples of domestic regulatory models in Africa. It develops a five-dimensional framework to evaluate how well domestic policies in each of these countries align with AfCFTA cross-border data flow obligations. It examines the legal foundations, regulatory scope, institutional mechanisms, rights and digital protections, and socio-economic and technical contexts. The AfCFTA Digital Trade Protocol and the Cross-Border Data Transfers Annex are seen as setting a general obligation to allow cross-border data transfers for digital trade, with specific treaty-based conditions and exceptions.

The thesis argues that the observed regulatory differences mainly show variations in institutional capacity, regulatory methods, and implementation order rather than deep legal conflicts. It proposes treaty-derived thresholds to separate legally significant incompatibility from acceptable regulatory differences. The thesis redefines digital trade integration under the AfCFTA through the lens of legal compatibility rather than requiring Uniform harmonization.

United Nations Sustainable Development Goals Connections

This thesis contributes to several United Nations Sustainable Development Goals by examining the legal governance of cross-border data flows under the African Continental Free Trade Area (AfCFTA) and its effects on digital trade integration, regulatory capacity, and institutional development in Africa. Its contributions directly relate to SDGs 8, 9, 10, 16, and 17, as detailed below.

1. *SDG 8 – Decent Work and Economic Growth*

- Target 8.2 (Achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high value added and labor-intensive sectors)
- Target 8.3 (Promote development-oriented policies that support productive activities, decent job creation, entrepreneurship, creativity and innovation, and encourage the formalisation and growth of micro-, small- and medium-sized enterprises, including through access to financial services)

Digital trade increasingly relies on firms, especially small and medium-sized enterprises, being able to transfer data across borders. By examining how AfCFTA cross-border data flow obligations can be enacted without requiring immediate or rigid legal harmonization, the thesis clarifies the legal conditions that allow African firms to engage in regional digital markets. The framework developed in this thesis fosters growth-focused digital trade by reducing legal uncertainty around data transfers while maintaining regulatory independence. This approach helps boost innovation, service exports, and involvement in digital value chains.

2. *SDG 9 – Industry, Innovation, and Infrastructure*

- Target 9.1 (Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all)
- Target 9.c (Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020)

Cross-border data flows form a fundamental part of digital infrastructure. This thesis addresses data governance as a legal infrastructure issue, showing how compatible legal frameworks enable digital connectivity across different jurisdictions. By presenting AfCFTA cross-border data flow governance as an interoperability system instead of a harmonization project, the thesis supports the creation of regionally connected digital infrastructure. This approach accounts for varying institutional capacities while ensuring legal predictability.

3. *SDG 10 – Reduced Inequalities*

- Target 10.2 (By 2030, empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status)
- Target 10.a (Implement the principle of special and differential treatment for developing countries, in particular least developed countries, in accordance with World Trade Organization agreements)

The thesis directly tackles the structural inequalities that stem from uneven regulatory and institutional capacities among African states. Its distinction between doctrinal incompatibility and capacity-based differences provides a legally sound foundation for allowing variation without reinforcing exclusion. By acknowledging capacity-sensitive implementation paths under AfCFTA

law, the thesis aligns with SDG 10's focus on inclusive integration and varied implementation within a shared legal framework.

4. *SDG 16 – Peace, Justice, and Strong Institutions*

- Target 16.3 (Promote the rule of law at the national and international levels and ensure equal access to justice for all)
- Target 16.6 (Develop effective, accountable and transparent institutions at all levels)

A key contribution of this thesis is its enhancement of legal clarity and institutional accountability in the governance of cross-border data flows. By pinpointing treaty-based thresholds for legal incompatibility and clarifying the extent of acceptable regulatory variation, the thesis supports the implementation of AfCFTA obligations grounded in the rule of law. Its focus on clear regulatory criteria and careful application of public policy exceptions aids in building predictable and accountable legal institutions at both national and continental levels.

5. *SDG 17 – Partnerships for the Goals*

- Target 17.10 (Promote a universal, rules-based, open, non-discriminatory and equitable multilateral trading system under the World Trade Organization, including through the conclusion of negotiations under its Doha Development Agenda)
- Target 17.14 (Enhance policy coherence for sustainable development)

The AfCFTA serves as a vital tool for regional partnership in Africa. This thesis contributes to SDG 17 by showing how policy coherence in digital trade can be achieved through legal interoperability instead of uniformity. Its analysis encourages regulatory cooperation, mutual understanding, and coordinated efforts among African states, strengthening AfCFTA's role as a rules-based framework for regional integration in line with broader multilateral trade principles.

Statement of Original and Disclosure of Use of Artificial Intelligence

In accordance with the *Guidelines for AI Use in Graduate Research* and Queen's University academic integrity policies, the author used artificial intelligence–assisted tools in a limited and transparent manner during the research and writing of this thesis. Specifically, *OpenAI's ChatGPT* and *Grammarly* were used as assistive tools for language refinement, structural clarity, and conceptual clarification during drafting and revision. These tools were not used to produce original legal analysis, arguments, or conclusions. All content included in this thesis was written, reviewed, and finalized by the author, who accepts full responsibility for its accuracy, originality, and scholarly integrity.

Acknowledgement

I am profoundly thankful to Allah, whose grace enabled me to pursue and complete my LL.M. journey. I appreciate my family for their unwavering encouragement and support throughout this process. My sincere gratitude goes to my supervisor, Professor Nicolas Lamp, for his guidance, engagement, and constructive feedback at every stage of my LL.M., including this thesis. I also thank the members of my examination committee for their time, careful reading, and insightful comments. Additionally, I am grateful to Professor Joshua Karton, who taught the Legal Research Methods and Perspectives course, which enhanced my ability to formulate key questions and significantly influenced the focus and depth of my research. I also owe much appreciation to the Graduate Program Coordinator, Kate Black, whose professionalism, responsiveness, and steady support greatly eased my navigation through the LL.M. program.

Table of Contents

Abstract.....	ii
United Nations Sustainable Development Goals Connections.....	iii
Statement of Original and Disclosure of Use of Artificial Intelligence	vi
Acknowledgement.....	vii
Table of Contents.....	viii
Table of Statutes and Treaties	xiv
<i>Continental</i>	xiv
<i>Kenyan</i>	xiv
<i>Nigerian</i>	xiv
<i>South African</i>	xv
List of Abbreviations	xvi
Chapter 1: General Introduction	1
<i>1.1 Introduction</i>	1
<i>1.2 Contextual Background</i>	3
1.2.1 Cross-Border Data Flows (CBDF) in Digital Trade in Africa	3
1.2.2 CBDF Governance Challenge and the AfCFTA Digital Trade Protocol.....	5
<i>1.3 Aim and objectives</i>	7
<i>1.4 Research Questions</i>	8
1.4.1 Primary Research Question	9
1.4.2 Secondary Research Questions	9
<i>1.5 Scope of Research</i>	9
<i>1.6 Research Methodology</i>	10
<i>1.7 Thesis Structure</i>	12

Chapter 2: Literature Review and Analytical Framework.....	14
2.1 <i>Introduction</i>	14
2.2 <i>Literature Review on Digital Trade Law and Cross-Border Data Flows</i>	15
2.2.1 Legal Approaches to Cross-Border Data Flows in Digital Trade Agreements.....	16
2.2.2 Regulatory Fragmentation, Interoperability and Alignment in CBDF Governance	20
2.2.3 Existing Scholarship on CBDF Governance in Africa.....	22
2.3 <i>Limitations in Existing Scholarship</i>	26
2.4 <i>Analytical Framework for Assessing AfCFTA CBDF Alignment</i>	27
2.4.1 Legal-Normative Foundations.....	28
2.4.2 Substantive Regulatory Scope.....	28
2.4.3 Institutional and Implementation Mechanisms	29
2.4.4 Rights and Digital Safeguards.....	29
2.4.5 Socio-Economic and Technical Context	29
2.5 <i>Operationalization of the Framework</i>	30
2.6 <i>Conclusion</i>	32
Chapter 3: Legal Architecture of CBDF Under the AfCFTA Digital Trade Protocol and its CBDF Annex	34
3.1 <i>Introduction</i>	34
3.2 <i>Legal Status and Scope</i>	35
3.3 <i>Normative Foundations of CBDF under the AfCFTA Digital Trade Protocol</i>	37
3.4 <i>Substantive Disciplines Governing CBDF</i>	39
3.4.1 Cross-Border Data Transfer Obligations and Scope	39
3.4.2 Data Localisation and Computing Facilities Requirements	40
3.4.3 Non-Discrimination, Equivalence, and Transfer Conditions	41
3.4.4 Transfer Mechanisms and Regulatory Cooperation	42
3.4.5 The AfCFTA CBDF Benchmark.....	42

3.5	<i>Exceptions, Safeguards and Regulatory Autonomy</i>	43
3.5.1	Public Policy and Essential Security Exceptions.....	43
3.5.2	Privacy, Data Protection, and Trust-Based Safeguards	44
3.5.3	Institutional Safeguards and Cooperative Mechanisms.....	45
3.5.4	Implications for the AfCFTA CBDF Benchmark	45
3.6	<i>Institutional Framework and Implementation Arrangements</i>	45
3.6.1	Institutional Placement within the AfCFTA Framework	46
3.6.2	Cooperation and Information Exchange.....	47
3.6.3	Relationship to Dispute Settlement	48
3.6.4	Implications for the AfCFTA CBDF Benchmark	48
3.7	<i>Synthesis of the AfCFTA CBDF Benchmark</i>	49
Chapter 4: Domestic CBDF Regimes in Nigeria, Kenya, and South Africa.....		51
4.1.0	<i>Introduction</i>	51
4.2.0	<i>Nigeria</i>	53
4.2.1	Legal-Normative Foundations.....	55
4.2.2	Substantive Regulatory Scope.....	58
4.2.3	Institutional and Enforcement Mechanisms	62
4.2.4	Rights and Digital Safeguards.....	65
4.2.5	Socio-Economic and Technical Context	68
4.3.0	<i>Kenya</i>	69
4.3.1	Legal-Normative Foundations.....	71
4.3.2	Substantive Regulatory Scope.....	73
4.3.3	Institutional and Enforcement Mechanisms	75
4.3.4	Rights and Digital Safeguards.....	78
4.3.5	Socio-Economic and Technical Context	80
4.4.0	<i>South Africa</i>	82

4.4.1	Legal-Normative Foundations.....	83
4.4.2	Substantive Regulatory Scope.....	86
4.4.3	Institutional and Implementation Mechanisms	88
4.4.4	Rights and Digital Safeguards.....	90
4.4.5	Socio-economic and technical context.....	92
4.5.0	<i>Comparative Synthesis of Alignment and Misalignment</i>	94
4.6.0	<i>AfCFTA CBDF Alignment Scorecard and Diagnostic Findings</i>	98
4.7.0	<i>Conclusion</i>	102
Chapter 5: Towards Operationalizing the AfCFTA CBDF Regime		105
5.1.0	<i>Introduction</i>	105
5.2.0	<i>Structural Sources of CBDF Alignment</i>	108
5.2.1	Normative Layering and Legal Pluralism.....	108
5.2.2	Delegated Governance Density and Regulatory Technique.....	109
5.2.3	Institutional Asymmetry and Administrative Capacity	110
5.2.4	Trade–Privacy Interface and Regulatory Orientation	110
5.2.5	<i>Capacity Sensitivity and Multi-Level Normative Context</i>	111
5.3.0	<i>Doctrinal Conflicts versus Capacity-Based Implementation Gaps</i>	112
5.3.1	Doctrinal Incompatibility under the AfCFTA CBDF Framework	112
5.3.2	Capacity-Based and Implementation-Driven Divergence	113
5.3.3	The Legal Significance of the Distinction	115
5.3.4	Implications for Alignment Assessment.....	116
5.4.0	<i>Pathways for Operationalizing AfCFTA Obligations within Existing Domestic Framework</i>	116
5.4.2	Continental-Level Operational Support and Coordination.....	118
5.4.3	The Legal Limits of Operational Alignment	120
5.5.0	<i>Sequencing and Phasing of AfCFTA CBDF Implementation</i>	120
5.5.1	Legal Basis for Sequencing and Phasing of AfCFTA CBDF Implementation	121

5.5.2 Sequencing as a Compliance-Permissible Implementation Practice	121
5.5.3 Sequencing, Managed Divergence, and Alignment Assessment.....	122
5.5.4 Legal Limits of Sequencing under AfCFTA Law	122
5.5.5 Implications for Alignment Evaluation	123
5.6.0 <i>Implications for Continental Digital Trade Integration</i>	123
5.7.0 <i>Conclusion</i>	125
General Conclusion	127
Bibliography	131
<i>Primary Materials</i>	131
International Treaties	131
Legislations: Kenya	131
Legislation: Nigeria	131
Legislation: South Africa.....	132
<i>Secondary Sources</i>	132
Secondary Materials: Electronic Sources	134
Secondary Sources: Journal Articles	137
Secondary Materials: Newspaper	153
Secondary Materials: Reports.....	153
Secondary Materials: Thesis.....	158
Secondary Materials: Unpublished Manuscripts	159
Annex A – Coding Manual and Scoring Rules	162
<i>A.1 Purpose of the Coding Manual</i>	162
<i>A.2 Units of Analysis and Sources</i>	162
<i>A.3 AfCFTA CBDF Benchmark Mapping</i>	163
<i>A.4 Description of Analytical Dimensions, Coding Criteria and Anchor Thresholds</i>	163
<i>A.5 Scoring Rules and Constraints</i>	166

A.6 Scoring Workflow 166

A.7 Coding Log with Evidence 167

A.8 Evidence–Anchor Mapping (Anchor-Scale Traceability Table) 180

A.9 Use, Limits, and Replicability 183

Table of Statutes and Treaties

Continental

- Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade, adopted 18 February 2024.
- Annex on Cross-Border Data Transfers (adopted as an annex to the AfCFTA Digital Trade Protocol; compiled certified legal instruments version on AU site).
- Agreement Establishing the African Continental Free Trade Area (AfCFTA Agreement)

Kenyan

- Data Protection Act, No 24 of 2019
- Data Protection (Civil Registration) Regulations, Legal Notice No 196 of 2020
- Data Protection (General) Regulations, Legal Notice No 263 of 2021
- Data Protection (Complaints Handling Procedure and Enforcement) Regulations, Legal Notice No 264 of 2021
- Data Protection (Registration of Data Controllers and Data Processors) Regulations, Legal Notice No 265 of 2021

Nigerian

- Nigeria Data Protection Act, 2023
- Nigeria Data Protection Act—General Application and Implementation Directive (GAID) 2025
- Nigerian Communications Act, 2003, No 19.
- Central Bank of Nigeria (CBN) Revised Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry.

- Central Bank of Nigeria (CBN) Guidelines on Point of Sale (POS) Card Acceptance Services, 2011.
- Designation and Protection of Critical National Information Infrastructure Order, 2024
- Constitution of the Federal Republic of Nigeria, 1999 (as amended)

South African

- Cybercrimes Act, Act No 19 of 2020.
- National Cybersecurity Policy Framework of 2015.
- Protection of Personal Information Act (POPI Act), 2013.
- Regulations Relating to the Protection of Personal Information, 2018.
- Regulations Relating to the Protection of Personal Information, 2025.

List of Abbreviations

- CBDF – Cross Border Data Flows
- SADC – Southern African Development
- ECOWAS – Economic Community of West African States
- EU – European Union
- AU – African Union
- GDPR – General Data Protection Regulation
- POPIA – Protection of Personal Information Act
- AfFCTA – African Continental Free Trade Area
- BCR – Binding Corporate Rules
- SCC – Standard Contractual Clauses
- DPA – Data Protection Authority
- DTP – Digital Trade Protocol (of the African Continental Free Trade Area Agreement)
- TPP – Trans-Pacific Partnership
- CPTPP – Comprehensive and Progressive Agreement for Trans-Pacific Partnership
- IoT – Internet of Things
- AI – Artificial Intelligence
- MSMEs – Micro, Medium and Small-sized Enterprises
- IFC – International Financial Corporation
- WTO – World Trade Organization
- RECs -Regional Economic Communities

Chapter 1: General Introduction

1.1 Introduction

Digital transformation is changing how trade, production, and service delivery work in the global economy.¹ Nowadays, commercial activity relies not just on the movement of goods and money across borders but also on the constant flow of data between different regions.² From cloud services and digital payments to e-commerce platforms and remote services, cross-border data flows (CBDF) have become essential for modern trade.³ This shift has made data regulation a key issue in current trade governance, influencing market access, competitiveness, and economic integration.⁴ While international trade law has mainly focused on the movement of goods and services, the increasing importance of data in the economy has revealed gaps in current trade rules.⁵ This situation has heightened tensions between trade liberalisation, data protection, national security, and digital sovereignty.⁶

In Africa, these tensions are particularly pronounced.⁷ African states are simultaneously pursuing digital industrialization, expanding participation in global digital markets, and strengthening

¹ OECD, “Digital trade” (28 December 2024), online: *OECD* <<https://www.oecd.org/en/topics/digital-trade.html>>.

² See Joshua Paul Meltzer, “The Internet, Cross-Border Data Flows and International Trade” (2015) 2:1 *Asia & the Pacific Policy Studies* 90–102 at 92.

³ see Chin Yik-Chan & Jingwu Zhao, “Governing Cross-Border Data Flows: International Trade Agreements and Their Limits” (2022) 11:63 *Laws* 1–22 at 1.

⁴ See generally Joshua P Meltzer, “Governing Digital Trade” (2019) 18:S1 *World trade review* S23–S48 at s23–s24.

⁵ See Susan Ariel Aaronson, “Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows” (2018) 197 *CIGI Papers* at 8 Aaronson explains that the GATS is the most relevant WTO agreement for data-driven services, but it predates the internet/WWW and says nothing explicit about cross-border data flows, hence the regulatory gap.

⁶ See: Yik-Chan & Zhao, “Governing Cross-Border Data Flows”, *supra* note 3 at 5 and 15.

⁷ See generally *Cross-border data flows in Africa: Continental ambitions and political realities – ECDPM Discussion Paper 379*, by Melody Musoni, Poorva Karkare, & Chloe Teevan (EDPM) at 1–2 online: <<https://ecdpm.org/application/files/8417/3202/4662/Cross-Border-Data-Flows-Africa-Continental-Ambitions-Political-Realities-ECDPM-Discussion-Paper-379-2024.pdf>>.

domestic data governance frameworks.⁸ Over the last decade, many countries have adopted comprehensive data protection laws, cybersecurity regulations, and sector-specific data rules.⁹ While these developments have strengthened domestic regulatory capacity, they have also produced a diverse and uneven legal landscape governing cross-border data flows.¹⁰ African CBDF regimes are therefore widely characterized as fragmented by exhibiting divergent national regulatory choices rather than coordinated continental framework. This raises concerns about regulatory uncertainty, compliance costs, and barriers to continental digital trade integration.

At the continental level, the African Continental Free Trade Area (AfCFTA) represents the most ambitious attempt to address these challenges through coordinated trade governance.¹¹ The adoption of the AfCFTA Digital Trade Protocol (DTP), including its Annex on Cross-Border Data Flows, reflects an explicit recognition that digital trade and data governance are integral to African economic integration.¹² The Protocol seeks to establish a common legal framework for digital trade among State Parties while simultaneously affirming their right to regulate within their territories for legitimate public policy objectives, including privacy, security, and sustainable development.

⁸ See generally Francesca Casalini & Javier López González, “Trade and Cross-Border Data Flows” (2019) 220 OECD Trade Policy Papers (OECD Trade Policy Papers) , online: <https://www.oecd.org/en/publications/trade-and-cross-border-data-flows_b2023a47-en.html> at 1 volume: 220.

⁹ See Melody Musoni, Poorva Karkare, & Chloe Teevan, *supra* note 7 at 2–5.

¹⁰ See African Union, *Guidelines for Integrating Data Provisions in Protocols on Digital Trade* (2023), online: <https://au.int/sites/default/files/documents/44807-doc-Guidelines-Integrating-Data-Digital-Trade-ENG-V3_161.pdf> at 3–4.

¹¹ See Roberto Echandi, Maryla Maliszewska & Victor Steenbergen, “Making the Most of the African Continental Free Trade Area” (2022) World Bank Publications - Books, online: <<https://ideas.repec.org/b/wbk/wbpubs/37623.html>> at 1–4.

¹² See Franziska Sucker & Alexander Beyleveld, “African Rules on Cross-Border Data Flows: The Significance of Regulatory Convergence and the African Continental Free Trade Area’s Digital Trade Protocol’s Potential Contribution” in J Drexler, M Hennemann, & K Weidemann, eds, *Comparative Data Law MPI Studies on Intellectual Property and Competition Law* (Springer, Cham, 2023) 151 at 15.

Notably, the Digital Trade Protocol does not seek to replace domestic data governance regimes or establish a uniform African data protection code.¹³ Its scope and structure instead reflect a trade-law design that combines baseline digital trade commitments with carefully circumscribed public policy and security exceptions, alongside obligations requiring State Parties to adopt or maintain domestic legal frameworks for personal data protection.¹⁴ Read together, these provisions suggest that the AfCFTA digital trade regime operates not as a harmonisation instrument in the classical sense, but as a coordination framework that can constrain and structure regulatory divergence while preserving domestic regulatory autonomy.

Against this background, this thesis examines whether the AfCFTA Digital Trade Protocol can function as a legally credible and institutionally workable coordination framework for cross-border data flow governance in Africa. Rather than presuming full regulatory harmonisation, the thesis interrogates how AfCFTA-level frameworks interact with diverse domestic legal regimes, and what this reveals about the possibilities and limits of digital trade integration under conditions of persistent regulatory diversity.

1.2 Contextual Background

1.2.1 Cross-Border Data Flows (CBDF) in Digital Trade in Africa

Digital trade in Africa has expanded alongside improvements in digital connectivity, mobile infrastructure, and data-driven services. Cross-border data flows are a component of this growth.

They enable delivery of digitally supplied services, operation of cloud systems, coordination of e-

¹³ See *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* arts 2, 3 and 21. The objectives and scope of the agreement is framed as facilitating digital trade under AfCFTA, not as a comprehensive data governance or data protection instrument. Also, the Protocol requires State Parties to adopt or maintain a personal data protection framework consequently preserving national systems.

¹⁴ *Ibid* arts 20, 21, 25 and 26.

commerce platforms, and processing of digital payments across different regions.¹⁵ As a result, the exchange of personal, transactional, and commercial data has become an increasingly routine feature of economic activity across the continent.

This expansion has been driven in large part by the rapid growth of mobile broadband connectivity, which now accounts for the majority of internet access in many African countries.¹⁶ The increased availability of mobile internet has supported the development of digital services in sectors such as finance, retail, logistics, and professional services.¹⁷ At the same time, the underlying infrastructure for digital trade remains uneven. Fixed broadband penetration remains below global averages, high-speed connections are often concentrated in urban areas, and broadband costs in many countries exceed international affordability benchmarks when measured as a share of average monthly income.¹⁸ These constraints shape the scale, reliability, and reach of data-intensive digital services and influence how cross-border data flows are regulated in practice.

The growth of digital payments and e-commerce further illustrates the economic significance of CBDF in Africa.¹⁹ The continent hosts one of the world's largest mobile money markets, facilitating large volumes of digital transactions, including cross-border payments.²⁰ E-commerce platforms similarly depend on cross-border data exchanges for payment processing, fraud prevention, customer support, and logistics coordination.²¹ Together, these developments

¹⁵ Meltzer, *supra* note 2 at See 91.

¹⁶ See ITU & UNESCO, “The State of Broadband in Africa 2025”, online: <https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.32-2025-PDF-E.pdf?utm_source=chatgpt.com> at 8.

¹⁷ See *The Mobile Economy Africa 2025*, by GSMA, Zotero at 3 online: <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/?utm_source=chatgpt.com>.

¹⁸ See ITU & UNESCO, *supra* note 16 at 8. The report records that despite progress, usage and infrastructure gaps remain; broadband penetration is well below global averages, and disparities exist by region, income, and urban/rural status.

¹⁹ See: *Digital Economy Report 2019 Value Creation and Capture: Implications for Developing Countries*, by UNCTAD, Open WorldCat (Geneva: United Nations, 2019) at 17–19 online: <https://unctad.org/system/files/official-document/der2019_en.pdf> [*Digital Economy Report 2019*].

²⁰ See GSMA, *supra* note 17 at 6–8, 14–16.

²¹ *World Development Report 2021: Data For Better Lives*, by World Bank (Washington, D.C: World Bank Group, 2021) at 33–35 online: <<https://www.worldbank.org/en/publication/wdr2021>> [*World Development Report 2021*].

underscore the central role of data flows in Africa’s digital economy, while also highlighting disparities in infrastructure capacity and market readiness that condition national approaches to data governance.

1.2.2 CBDF Governance Challenge and the AfCFTA Digital Trade Protocol

The AfCFTA is a key institutional framework for trade integration in Africa.²² Since its entry into force in 2019, the AfCFTA has sought to reduce trade barriers and to enhance economic integration among member states.²³ As digitalisation increasingly shapes trade patterns, the regulatory scope of the AfCFTA has also expanded to include digital economy issue, most notably through the adoption of the AfCFTA Protocol on Digital Trade.²⁴

The Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade was adopted by African Union (AU) member states in February 2024,²⁵ and its eight annexes (including cross-border data transfers) were adopted by the AU Assembly in February 2025.²⁶ These texts are now publicly available as part of the AfCFTA legal package. However, the Digital Trade Protocol and annexes have not yet entered into force because they require ratification by at least 22 AfCFTA State Parties before becoming binding. Once that threshold is reached, the Protocol enters into force 30 days after the 22nd ratification, and ratifying States typically have a period (up to five years) to implement its provisions domestically.²⁷ As of early 2026, no official

²² See Kola O Odeku & Teron Rikhotso, “African Continental Free Trade Area (AfCFTA): An Impetus for Intra-African Trade Integration” (2023) 10:1 *Journal of African Foreign Affairs* 111–131 at 111.

²³ *Ibid.*

²⁴ Kholofelo Kugler, “The AfCFTA Digital Protocol A bird’s eye view” (14 July 2025), online: *International Institute for Sustainable Development* <<https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol>>.

²⁵ The official copy of the Protocol released by the Au confirms the adoption date. See: *AfCFTA Digital Trade Protocol*, *supra* note 13.

²⁶ Official Presentation by the Department of Trade, Industry and Competition of the Republic of South Africa confirms this date of ratification Ratification of the AfCFTA Protocols (2025), online: <https://www.thedtic.gov.za/wp-content/uploads/Ratification-AfCFTA-Protocols.pdf?utm_source=chatgpt.com> at 6.

²⁷ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 47; *Agreement Establishing the African Continental Free Trade Area*, 2018 art 27(2).

continental register indicates that the Digital Trade Protocol has reached the 22-State ratification threshold, though individual States, for example Nigeria, have reportedly ratified the Digital Trade Protocol in November 2025.²⁸ Meanwhile, the broader AfCFTA Agreement, the parent treaty under which the Digital Trade Protocol sits has been widely ratified, with around 49 out of 55 African Union members having ratified the AfCFTA Agreement.²⁹

Notwithstanding the adoption of AfCFTA-level digital trade framework, the governance of cross-border data flows in Africa remains primarily anchored in domestic legal systems.³⁰ Most African countries manage cross-border data flows through their own data protection laws, sector-specific regulations, or practices that existed before the Digital Trade Protocol.³¹ These national systems vary in scope, structure, enforcement, and regulatory approach.³² As a result, African CBDF regimes are sometimes characterized as fragmented, raising concerns about regulatory uncertainty, compliance costs, and potential barriers to continental digital trade integration.³³

Regulatory diversity does not, in itself, predetermine the success or failure of continental trade integration. The critical issue is not the mere existence of divergence among domestic CBDF regimes, rather, whether such divergence operates within a framework capable of structuring, constraining, and coordinating national regulatory choices in a manner consistent with AfCFTA

²⁸ Official report from the Nigeria Federal Ministry of Industry, Trade and Investment confirms the ratification of the AfCFTA Digital Trade Protocol in November 2025. See: *Nigeria AfCFTA Achievements Report 2025.*, by Nigeria Federal Ministry of Industry, Trade and Investment (Abuja, 2025) at 2. online: <<https://fmiti.gov.ng/wp-content/uploads/2026/01/Nigeria-AfCFTA-Achievements-2025.pdf>>.

²⁹ Tralac, “African Continental Free Trade Area (AfCFTA) Legal Texts and Policy Documents”, online: *Tralac trade law centre* <https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html?utm_source=chatgpt.com>.

³⁰ See Franziska Sucker & Alexander Beyleveld, “African rules on cross-border data flows: The significance of regulatory convergence and the AfCFTA Digital Trade Protocol’s potential contribution” in *Comparative Data Law MPI Studies on Intellectual Property and Competition Law* (Switzerland: Springer Nature Switzerland, 2024) at 154.

³¹ See *ibid* at 169.

³² See *ibid* at 160.

³³ *ibid*

commitments.³⁴ Although the Digital Trade Protocol and its annexes require ratification and domestic implementation before becoming fully operational, their adoption provides the relevant legal context for assessing how AfCFTA framework may interact with, and shape, national approaches to cross-border data flow governance.

This study examines how diverse national regimes interact with the emerging digital trade rules under the AfCFTA, especially how commitments on the cross-border data flow can serve as a practical coordination framework for managing regulatory divergence without undermining local control over data policy.

1.3 Aim and objectives

The primary aim of this thesis is to assess the extent to which domestic legal frameworks governing cross-border data flows in selected African states are compatible with, and capable of being coordinated through, the commitments established under the AfCFTA Digital Trade Protocol. Rather than treating alignment as legislative uniformity or assuming the full operationalization of AfCFTA digital trade disciplines, the thesis evaluates how AfCFTA-level CBDF commitments structure, constrain, and orient domestic regulatory choices, and what this implies for effective digital trade integration under conditions of persistent regulatory diversity. To achieve this aim, the thesis pursues the following specific objectives:

1. To identify and clarify the core cross-border data flow obligations, exceptions, and regulatory safeguards contained in the AfCFTA Digital Trade Protocol and its Annex, and to distil these elements into a coherent benchmark for comparative assessment.

³⁴ As Chin and Zhao suggest, CBDF governance depends on whether international rules can reconcile regulatory autonomy with trade commitments through structured constraints and safeguards. See: Yik-Chan & Zhao, “Governing Cross-Border Data Flows”, *supra* note 3 at 14-16.

2. To examine the domestic legal frameworks governing cross-border data flows in Nigeria, Kenya, and South Africa, with particular attention to their legal foundations, regulatory scope, institutional arrangements, and rights-based protections.
3. To assess the degree and nature of compatibility between domestic CBDF regimes and AfCFTA-level commitments, distinguishing between doctrinal inconsistency, permissible regulatory variation, and implementation-related gaps.
4. To analyse how differences in domestic regulatory design and enforcement capacity affect the prospective operation of AfCFTA digital trade disciplines, particularly in relation to trust-based cross-border data flows.
5. To identify legally and institutionally realistic pathways for improving coordination and implementation of AfCFTA CBDF commitments, while preserving domestic regulatory autonomy and acknowledging capacity constraints among State Parties.

By pursuing these objectives, the thesis contributes a structured comparative legal analysis of CBDF governance that is explicitly grounded in AfCFTA treaty commitments, while operationalising those commitments through a multi-dimensional analytical framework informed by the comparative digital trade literature. In doing so, it offers an approach to understanding how continental digital trade disciplines may function across diverse national legal systems without presuming full regulatory harmonisation.

1.4 Research Questions

Flowing from the research problem identified above and the study's objectives, this thesis is guided by the following research questions:

1.4.1 Primary Research Question

- How do the AfCFTA Digital Trade Protocol and its Annex on Cross border data flow discipline and coordinate the governance of cross-border data flows in Africa, given the diversity of existing domestic legal regimes?

1.4.2 Secondary Research Questions

To answer the primary research question, the thesis addresses the following subsidiary questions:

- How do the domestic legal frameworks of Nigeria, Kenya, and South Africa regulate cross-border data flows in terms of legal foundations, regulatory scope, institutional arrangements, and rights-based protections?
- In what ways do domestic CBDF regimes align with, diverge from, or fall outside the commitments established under the AfCFTA Digital Trade Protocol, and how can these differences be characterized whether as doctrinal inconsistency, permissible regulatory variation, or implementation-related gaps?
- How do differences in domestic regulatory design and enforcement capacity shape the prospective interaction between AfCFTA-level digital trade commitments and national CBDF governance frameworks?
- What pathways do the AfCFTA Digital Trade Protocol and its institutional architecture make available for coordinating domestic CBDF regimes while preserving regulatory autonomy and accounting for capacity constraints among State Parties?

1.5 Scope of Research

This thesis focuses exclusively on trade-related aspects of cross-border data flows as they arise within the AfCFTA framework. It does not provide a comprehensive account of domestic data

governance, nor does it evaluate non-trade-related dimensions such as surveillance practices, data ethics, or sector-specific data regulation. Economic impact assessments and quantitative trade modelling are also beyond the scope of the analysis. By delimiting its scope in this manner, the thesis maintains analytical focus and avoids overstating the regulatory reach of AfCFTA instruments.

1.6 Research Methodology

This thesis adopts a qualitative comparative legal methodology grounded in doctrinal analysis and structured benchmarking. It examines the governance of cross-border data flows through a close reading of treaty texts, domestic legislation, regulatory instruments, and relevant jurisprudence, supplemented by authoritative secondary literature on digital trade and data governance. The methodological focus is on legal structure, normative orientation, and regulatory interaction, rather than on empirical measurement of economic outcomes or post-implementation compliance.

The comparative analysis focuses on Nigeria, Kenya, and South Africa. These jurisdictions are selected because they represent leading African data governance regimes with differing legal traditions, institutional capacities, and regulatory approaches to cross-border data flows. Together, they provide analytically useful contrasts for examining how diverse domestic legal systems interact with AfCFTA-level digital trade commitments.

Given the emergent and phased nature of the AfCFTA Digital Trade Protocol, this thesis does not assess compliance or enforcement outcomes. Instead, it evaluates the prospective compatibility and coordination potential of existing domestic CBDF regimes in light of AfCFTA-level commitments. The analysis therefore treats AfCFTA disciplines as normative reference points that structure future legal expectations, rather than as operational rules that already govern domestic

regulatory practice. This approach reflects orthodox methods in international economic law, where legal analysis routinely examines treaty obligations and regulatory interaction prior to full domestic implementation.

To operationalise this assessment, the thesis constructs an AfCFTA-centred benchmark derived from the substantive architecture of the Digital Trade Protocol and its Annex on Cross-Border Data Flows. This benchmark is grounded in binding treaty obligations, scope provisions, exceptions, regulatory safeguards, and institutional arrangements relevant to trade-related data governance. It does not assume regulatory uniformity or full legal harmonization but instead identifies the outer parameters within which domestic regulatory diversity may lawfully persist.

The benchmark is applied through a five-dimension analytical framework that organizes the comparative assessment across key aspects of CBDF governance: legal and normative foundations; transfer mechanisms and localization constraints; enforcement and institutional capacity; regional and international regulatory alignment; and compatibility with AfCFTA digital trade disciplines. While the substantive content of the benchmark is derived from AfCFTA treaty commitments, the structuring of these dimensions is informed by the comparative digital trade and data governance literature. The framework thus serves as an analytical instrument that translates AfCFTA-level disciplines into assessable criteria, without importing external normative models or evaluating regulatory quality as such.

Comparative findings are presented using structured qualitative assessment, supported where appropriate by anchor-scale indicators to illustrate degrees and types of compatibility. These indicators are used to distinguish between doctrinal inconsistency, permissible regulatory variation, and implementation-related gaps. They are not intended to measure compliance,

effectiveness, or regulatory success, but to facilitate transparent and consistent comparison across jurisdictions.

Through this methodological approach, the thesis seeks to provide a disciplined legal analysis of how AfCFTA-level digital trade commitments may orient, constrain, and coordinate domestic cross-border data flow regimes over time, while acknowledging the continued relevance of domestic regulatory autonomy and capacity constraints.

1.7 Thesis Structure

This thesis is organized into five substantive chapters, followed by a general conclusion, each of which addresses the research problem, questions, and objectives outlined in this chapter.

Chapter 1 introduces the study by situating cross-border data flows within the broader context of digital trade and continental integration in Africa. It sets out the research problem, aim, objectives, research questions, scope, and methodology that guide the analysis.

Chapter 2 reviews the existing literature on digital trade, cross-border data flow governance, and regulatory alignment, with particular attention to African perspectives. Building on this review, the chapter develops the analytical framework used in the thesis, identifies the five dimensions for assessing domestic CBDF regimes, and explains the operationalization of the framework.

Chapter 3 examines the AfCFTA Digital Trade Protocol and the Annex on Cross-Border Data Transfers as a legal benchmark. It analyses the structure, objectives, and core obligations of the AfCFTA CBDF regime, including permissible public policy exceptions, to establish the continental standards against which domestic legal frameworks are evaluated.

Chapter 4 applies the analytical framework to a comparative examination of domestic CBDF regimes in Nigeria, Kenya, and South Africa. The chapter analyses each case study across the five

dimensions of the framework, identifies areas of alignment and misalignment with AfCFTA commitments, and synthesizes these findings through a comparative scorecard and diagnostic assessment.

Chapter 5 builds on the comparative findings to explore pathways for operationalizing the AfCFTA CBDF regime. It distinguishes between doctrinal conflicts and capacity-based implementation gaps, examines institutional and regulatory constraints, and proposes legally realistic approaches to improving alignment while accommodating regulatory diversity among State Parties.

The **General Conclusion** synthesizes the thesis's findings, directly answers the research questions, reflects on the study's contribution and limitations, and offers brief forward-looking observations on the future of cross-border data flow governance under AfCFTA.

Chapter 2: Literature Review and Analytical Framework

2.1 Introduction

This chapter examines the academic and policy literature on managing cross-border data flows (CBDF) in digital trade and regional economic integration. It also develops the analytical framework used in the thesis. This chapter has two main functions. First, it outlines the key legal and conceptual debates shaping current approaches to CBDF regulation, focusing on trade law perspectives, regulatory coordination, and African scholarship. Second, it uses the limitations identified in the literature to build a structured analytical framework for assessing the alignment between domestic CBDF systems and the AfCFTA Digital Trade Protocol.

The literature review does not aim to be a comprehensive overview of all writings on data governance or digitization. Instead, it focuses selectively on scholarship that directly relates to the research problem identified in Chapter 1. This includes how cross-border data flows are regulated within trade frameworks, how regulatory differences and coordination are viewed, and how these issues have been discussed in African legal and policy settings. The review is organized thematically. It moves from global legal approaches to CBDF in digital trade agreements, to discussions of fragmentation and interoperability, and then to African-specific scholarship on data governance and regional integration.

The aim of this review is not to settle these debates but to clarify the analytical landscape in which the thesis is situated and to identify limitations in current approaches. The literature tends to discuss CBDF governance either at a high level of abstraction or through policy recommendations, with little focus on systematic, legally grounded assessments of how continental trade commitments align with domestic regulatory frameworks.

Based on this, the chapter develops the analytical framework used in the thesis. This framework allows for a structured assessment of the alignment between AfCFTA CBDF commitments and domestic legal frameworks. It does not assume regulatory harmonization, nor view divergence as a problem. The latter sections of the chapter outline the framework and its application, providing the methodological basis for the comparative analysis in the following chapters.

2.2 Literature Review on Digital Trade Law and Cross-Border Data Flows

The management of cross-border data flows (CBDF) has become a major issue in today's digital trade law.³⁵ As data becomes crucial for producing and delivering goods and services, legal rules governing its international movement increasingly influence market access, regulatory independence, and the structure of digital economic integration.³⁶ Scholars from various fields, including international trade law, data protection law, and global economic governance, all engage with CBDF governance. Much of this legal scholarship focuses on how trade agreements and related regulations strike a balance between facilitating data flows and maintaining legitimate public policy goals.

This literature review looks at three connected areas of scholarship related to the research problem discussed in this thesis. First, it explores legal approaches to cross-border data flows as seen in digital trade agreements and trade-related regulations, paying special attention to how these instruments define data flows, structure obligations, and allow for public policy exceptions. Second, it discusses conceptual debates about regulatory fragmentation, interoperability, and alignment in CBDF governance, which present differing views on how legal differences across jurisdictions affect cross-border digital trade. Third, it reviews existing legal and policy studies on

³⁵ Francesca Casalini & Javier López González, *supra* note 8 at 8.

³⁶ See *ibid* at 8–9.

CBDF governance in Africa, showing how both continental and national approaches have been examined in relation to regional integration efforts.

The aim of this review is not to judge among differing policy preferences or to recommend ideal data governance models. Instead, it aims to outline the analytical framework for CBDF governance, identify recurring assumptions and limitations in current approaches, and clarify how regulatory alignment questions are presented in the literature. By placing the study within these discussions, the review lays the groundwork for identifying limitations in existing scholarship and developing the analytical framework used in the following sections of this chapter.

2.2.1 Legal Approaches to Cross-Border Data Flows in Digital Trade Agreements

Legal scholarship on cross-border data flows (CBDF) has mainly progressed through the growth of digital trade agreements and trade-related regulations. As data has become essential for producing and delivering digitally enabled goods and services, international trade law today has had to tackle regulatory questions that earlier trade systems largely ignored. Scholars often point to the rise of CBDF governance in trade law as a response to the shortcomings of the multilateral trading system. They note that the World Trade Organization (WTO) framework did not address cross-border data transfers due to the historical divide between trade regulation and information governance.³⁷

In this context, legal analysis has examined how bilateral, regional, and plurilateral trade agreements have incorporated rules for data flows. Mira Burri has been particularly influential, arguing that data flows challenge traditional trade-law categories.³⁸ They blur the lines between goods and services, and directly link regulatory concerns to market-access conditions. From this

³⁷ Mira Burri, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation” (2017) 51 UC Davis Law Review 65–133 at 85–91.

³⁸ See generally Mira Burri, “The Impact of Digitalization on Global Trade Law” (2023) 24 German Law Journal 551–573 at 6–10.

viewpoint, CBDF provisions are not minor innovations; they represent a major shift in how trade law relates to the digital economy.³⁹

A key theme in the literature is the legal structure through which trade agreements manage CBDF. Studies of agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States–Mexico–Canada Agreement (USMCA), and specific digital economy agreements show a common trend. Commitments to allow cross-border data transfers often come with broad public-policy exceptions. This framework is frequently labelled as a “free flow of data with exceptions” model, which tries to balance trade liberalization with domestic regulatory freedom.⁴⁰ Mira Burri emphasizes the legal complexity of CBDF disciplines in trade agreements. She points out that broad and open-ended exception clauses can lead to legal uncertainty.⁴¹ This makes it unclear how reconciliation mechanisms would work in practice and, as a result, weakens confidence in enforceability in dispute settlement.

In this ongoing discussion, scholars have explored the different regulatory philosophies behind digital trade agreements. Henry Gao describes today’s digital trade governance as divided into three main “digital kingdoms”: a market-oriented model that prioritizes data mobility, a sovereignty-oriented model that emphasizes state control over data, and a rights-oriented model focused on privacy and data protection.⁴² Gao’s framework highlights the lack of a single dominant

³⁹ Burri, *supra* note 37 at 110–117.

⁴⁰ Susan Aaronson, “Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security” (2015) 14:4 *World Trade Review* 671–700 at 548–552; Mira Burri & Rodrigo Polanco, “Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset” (2020) 23:1 *J Int Economic Law* 187–220 at 203–207.

⁴¹ Mira Burri, “Cross-border data flows and privacy in global trade law: has trade trumped data protection?” (2023) 39:1 *Oxford Review of Economic Policy* 85–97 at 91–92, especially where she explains that the CPTPP-style public policy exception, without an enumerated list, can lead to “overall legal uncertainty” until precedents emerge. She also explains that it is unclear how layered general exceptions would work in practice, and that the privacy exception in GATS has never been tested in WTO dispute settlement.

⁴² Henry S Gao, “Data Sovereignty and Trade Agreements: Three Digital Kingdoms” (2021) *SSRN Journal*, online: <<https://www.ssrn.com/abstract=3940508>> at 5–12.

approach to CBDF in international trade law and emphasizes the coexistence of competing regulatory perspectives within and between agreements.

Building on these conceptual discussions, empirical and policy-focused research has worked to implement CBDF governance by pinpointing the specific legal methods states use to influence data movement. OECD analyses, particularly by Casalini and López González, chart data-related trade measures across jurisdictions.⁴³ They differentiate between data localization requirements, conditional transfer mechanisms, sector-specific restrictions, and regulatory safeguards. This research shows that CBDF governance functions along a spectrum of regulatory actions rather than a simple choice between openness and restriction. It offers a useful framework that informs discussions on trade law and trade policy without assuming agreement on a single regulatory model.

Concerns about regulatory autonomy and control over data have also influenced critical views on data localization and transfer restrictions. Anupam Chander and Uyên Lê argue that data localization often imposes substantial economic and trade costs while providing uncertain benefits in privacy or security.⁴⁴ Similarly, Nigel Cory has studied the trade-restrictive impacts of localization requirements, highlighting their potential to fragment digital markets and create barriers to cross-border services.⁴⁵ He warns against viewing these measures as automatically illegitimate from a public policy perspective.

Alongside these trade-focused discussions, legal scholarship has highlighted the link between CBDF governance and data-protection standards. Paul Schwartz has argued that data-protection

⁴³ See generally Francesca Casalini & Javier López González, *supra* note 8 at 9–22; See also Janos Ferencz, “The OECD Digital Services Trade Restrictiveness Index” (2019) 221 OECD Trade Policy Papers (OECD Trade Policy Papers), online: <<https://ideas.repec.org/p/oec/traaab/221-en.html>> at 15–21.

⁴⁴ See Anupam Chander & Uyên Lê, “Data Nationalism” (2015) 64:3 Emory Law Journal 678–739 at 83–112.

⁴⁵ *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, by Nigel Cory, ResearchGate (Information Technology and Innovation Foundation, 1 May 2017) [*Cross-Border Data Flows*].

laws increasingly act as de facto trade tools by influencing the conditions under which data can move across borders.⁴⁶ Christopher Kuner also places international data-transfer regulations at the crossroads of trade law and privacy law, emphasizing the challenges of aligning trans-border data flows with differing national standards for rights protection and regulatory oversight.⁴⁷

From a wider trade-law viewpoint, scholars like Joel P. Trachtman⁴⁸ and Panagiotis Delimatsis⁴⁹ have placed CBDF rules within theories of regulatory cooperation and managed diversity. Their works emphasizes that modern trade law does not aim to erase regulatory differences but to manage their effects across borders through flexible obligations, exceptions, and coordination mechanisms. This perspective supports the idea that CBDF provisions in trade agreements are better understood as tools for facilitating regulatory engagement rather than promoting regulatory uniformity.

Overall, this body of scholarship shows that digital trade agreements interact with cross-border data flows through various and often conflicting legal frameworks. Instead of converging toward a single regulatory model, trade law reflects an ongoing effort to balance data mobility, regulatory independence, and rights protection through adaptable, context-sensitive legal structures. These discussions offer a needed conceptual basis for examining how developing trade frameworks, such as the AfCFTA, will address CBDF governance and how domestic legal systems may either align with or differ from these approaches.

⁴⁶ See Paul M Schwartz, “Information Privacy in the Cloud” 161 *University of Pennsylvania Law Review* 1623–1662 at 1623–1624; See also Karl-Nikolaus Peifer, “Transatlantic Data Privacy Law” 106 *Georgetown Law Journal* at 121–129.

⁴⁷ See generally Christopher Kuner, *Transborder Data Flow Regulation and Data Privacy Law* (Oxford, United Kingdom: Oxford University Press, 2013) at 33–41.

⁴⁸ See generally Joel P Trachtman, “Trade and... Problems, Cost-Benefit Analysis and Subsidiarity” (1998) 9 *European Journal of International Law* at 33–35; 36–37.

⁴⁹ See generally P Delimatsis, “Determining the Necessity of Domestic Regulations in Services: The Best is Yet to Come” (2008) 19:2 *European Journal of International Law* 365–408 at 365–368; 386–387.

2.2.2 Regulatory Fragmentation, Interoperability and Alignment in CBDF Governance

A recurring theme in the cross-border data flows literature is that divergent domestic legal approaches create persistent governance tensions for cross-border digital activity.⁵⁰ Scholars frequently characterize the CBDF rule environment as fragmented, in the sense that states adopt differing (and sometimes conflicting) rules on data localization/storage requirements, the conditions for cross-border transfers, and the scope of rights and regulatory protections. Rather than treating fragmentation as a settled diagnosis, much of the trade-law scholarship frames it as an ongoing risk associated with reconciling data free-flow commitments with locally grounded regulatory frameworks and safeguards designed to preserve regulatory autonomy for privacy, security, and other public policy objectives.

In trade-law studies, regulatory fragmentation is often seen as a structural challenge, not a failure of governance. Joel P. Trachtman notes that trade regimes have traditionally operated in environments with regulatory diversity.⁵¹ Their purpose has been more about managing the effects of these differences than eliminating them altogether. From this angle, CBDF governance extends familiar trade-law challenges into a new regulatory area, rather than representing a fundamentally different breakdown of legal order.

In light of this, scholars have put forth various ways to respond to the regulatory diversity in CBDF governance. One response focuses on harmonization, which means adopting similar rules across jurisdictions. While harmonization has been a significant topic in policy discussions, legal scholars have increasingly questioned its practicality and appeal in data governance due to deeply rooted differences in constitutional traditions, regulatory priorities, and institutional capabilities. Graham

⁵⁰ See: Aaronson, “Why Trade Agreements are not Setting Information Free”, *supra* note 40 at 673–678.

⁵¹ See generally Joel P Trachtman, “The Future of International Law: Global Government” in Joel P Trachtman, ed, *The Future of International Law: Global Government* ASIL Studies in International Legal Theory (Cambridge: Cambridge University Press, 2013) v at 33–35; 36–37.

Greenleaf's comparative study of global data protection laws shows that approaches to data governance vary widely, even among regions that share common values, indicating structural limits to solutions based on uniformity.⁵²

Another response highlights interoperability, a concept related to mechanisms that allow different regulatory systems to work together without the need for identical rules. Kalypso Nicolaïdis has played a key role in developing models of "managed mutual recognition," where legal diversity is accommodated through procedures, equivalence assessments, and coordination mechanisms instead of harmonization.⁵³ In CBDF governance, interoperability aims to ease the movement of cross-border data while maintaining regulatory autonomy, but this often relies on high levels of institutional trust and cooperation.

A third area in the literature emphasizes alignment as a more adaptable analytical and regulatory idea. Unlike harmonization, alignment does not assume uniform rules, and unlike interoperability, it does not need formal mutual recognition. Instead, alignment looks at how compatible the regulatory goals, legal structures, and implementation practices are across different jurisdictions. OECD analyses, especially those considering data-related trade restrictions, implicitly adopt this method by evaluating how various regulatory techniques work together in practice, rather than measuring compliance against a single standard.⁵⁴

In trade-law studies, alignment has served as both a descriptive and evaluative framework for looking at how different legal systems coexist within broader trade structures. Scholars like Panagiotis Delimatsis have pointed out the importance of regulatory cooperation and coordination

⁵² Graham Greenleaf, "Global Data Privacy Laws: 89 Countries, and Accelerating" (6 February 2012) Rochester, NY, online: <<https://papers.ssrn.com/abstract=2000034>> at 1–4.

⁵³ See Kalypso Nicolaidis & Gregory Shaffer, "Transnational Mutual Recognition Regimes: Governance without Global Government" (2005) 68:3 *Law and Contemporary Problems* 263–318 at 261–271.

⁵⁴ Francesca Casalini & Javier López González, *supra* note 8.

in managing cross-border effects without eliminating domestic legal choices.⁵⁵ The WTO-focused literature emphasizes the existence of flexible rules and exception-based governance in areas sensitive to regulation. In this context, alignment acts more as an analytical tool than a prescriptive goal for understanding how legal systems function together in an integrated trade environment.⁵⁶ Overall, this body of literature suggests that discussions about fragmentation, interoperability, and alignment illustrate different views on how to handle regulatory diversity in CBDF governance. Instead of presenting a single solution, the scholarship reveals a range of approaches, each with its own legal and institutional impacts. These discussions lay the groundwork for evaluating how domestic CBDF systems interact with trade commitments and informing the choice to assess alignment later in this chapter, without assuming either convergence or fragmentation as an outcome.

2.2.3 Existing Scholarship on CBDF Governance in Africa

Scholarship on cross-border data flow governance in Africa has expanded alongside the growth of digital trade, the spread of domestic data protection frameworks, and renewed efforts toward continental digital integration. This literature spans trade law analysis, data protection and cybersecurity studies, and policy-oriented research on digital development. A recurring concern across these strands is how African states can advance digital trade integration while managing regulatory constraints, uneven institutional capacity, and competing priorities relating to privacy, security, and economic development.

One prominent strand of this scholarship examines the legal and policy tools available for regulatory coordination in African data governance. In this context, the African Union Convention

⁵⁵ See generally Panos Delimatsis, “Global Trade-Enabling Law” (2021) 13 *Indian Journal of International Economic Law*, online: <<https://papers.ssrn.com/abstract=4029104>> at 124.

⁵⁶ See generally “The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade” (2019) 18 *World Trade Review* 1–22.

on Cyber Security and Personal Data Protection (Malabo Convention) is frequently cited as an early continental initiative aimed at articulating shared principles on data protection and cybersecurity.⁵⁷ At the same time, scholars caution against assuming that the existence of continental instruments alone ensures effective regulatory alignment, emphasizing instead the significance of ratification patterns, domestic legal translation, and institutional strength.⁵⁸ Similar caution informs discussions of the AU Data Policy Framework, which, while recognized as an important normative reference point, is explicitly non-binding and dependent on domestic uptake and political-institutional context for its practical effect.

Another growing body scholarship situates CBDF governance within Africa's broader project of regional digital trade integration, including the AfCFTA's emerging digital trade framework.⁵⁹ Scholars disagree about the appropriate balance between liberalizing CBDF commitments and preserving regulatory space to support digital inclusion, trust, and domestic policy objectives in developing contexts.⁶⁰ Some caution that binding, highly liberal CBDF disciplines, if not paired with clear exceptions and capacity-sensitive design, may constrain institution-building and policy choices needed in lower-capacity regulatory environments.⁶¹ Others argue that regional coherence and interoperability in data governance can strengthen legal certainty for cross-border digital

⁵⁷ See: Graham Greenleaf & Bertil Cottier, "Comparing African Data Privacy Laws: International, African and Regional Commitments" (2020) 32 SSRN Journal, online: <<https://www.ssrn.com/abstract=3582478>> at 14.

⁵⁸ James Gathii emphasises limits of formalism, importance of implementation, and institutional capacity. James Thuo Gathii, *African Regional Trade Agreements as Legal Regimes*, 1st edn (Cambridge: Cambridge University Press, 2011) Cambridge International Trade and Economic Law at 580–584.

⁵⁹ See generally Neha Mishra & Kholofelo Kugler, "International Community in the Global Digital Economy: a Case Study on the African Digital Trade Framework" (2024) 73:4 International & Comparative Law Quarterly 853–889 at 853–859; María Vásquez Callo-Müller & Franziska Sucker, "Evolving approaches to cross-border data flows: Latin American and African perspectives" (2025) 00:00 International Data Privacy Law 1–16 at 1–17.

⁶⁰ See Andrew D Mitchell & Neha Mishra, "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute" (2019) 22:3 J Int'l Econ L 389–416 at 416; Yik-Chan & Zhao, "Governing Cross-Border Data Flows", *supra* note 3 at 2.

⁶¹ See Mitchell & Mishra, "Regulating Cross-Border Data Flows in a Data-Driven World", *supra* note 60 at 414–514; Mishra & Kugler, "International Community in the Global Digital Economy", *supra* note 59 at 879–880.

activity and help articulate shared African priorities in external digital trade rulemaking.⁶² Gathii's critique of African regional integration provides a useful lens, emphasizing how unequal partners and implementation realities (including flexibility and differentiated timetables) can strongly shape how agreements function in practice.⁶³

A third group of studies points out the gap between formal legal commitments and actual regulatory practices. The literature shows that enforcement can remain inconsistent in practice due to limited capacity and institutional constraints, even where legal frameworks and formal alignment with global norms exist.⁶⁴ Complementing this, cross-border data policy work by Research ICT, highlights that cross-border data governance debates on the continent are conditioned by infrastructure readiness, skills and administrative capacity, and the institutional foundations needed to sustain credible enforcement.⁶⁵ These literatures warns against analysis that relies solely on legal texts, stressing that cross-border data environment depends on both institutional performance and technical capability, not just formal regulatory alignment.⁶⁶

Lastly, comparative data protection research places African CBDF governance within a wider context of regulatory diversity across the continent Pan-African surveys and comparative analyses show substantial cross-jurisdictional variation in the scope of protections, institutional design, and enforcement tools, creating a fragmented compliance environment for actors operating across

⁶² Mishra & Kugler, "International Community in the Global Digital Economy", *supra* note 59 at 881–882.

⁶³ James Thuo Gathii, *African Regional Trade Agreements as Legal Regimes*, 1st edn (Cambridge: Cambridge University Press, 2011) Cambridge International Trade and Economic Law at 564.

⁶⁴ See Isaac Juma & Bukola Faturoti, "Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice" (2025) *International Review of Law, Computers & Technology* 1–26 at 12–13.

⁶⁵ See generally Alison Gillwald et al, *African Data and Digital Dialogues Report: Synthesis of the First and Second Knowledge Dialogue Workshops* (2022).

⁶⁶ See *Cross-border data flows in Africa: An analysis of the alignment with AfCFTA*, by Sandra Makumbirofa, Jackline Akello, & Nawal Omar (Cape Town: Research ICT Africa, 2025) at 4 online: <<https://researchictafrica.net/research/cross-border-data-flows-in-africa-an-analysis-of-the-alignment-with-afcfta/>> [*Cross-border data flows in Africa*].

borders.⁶⁷ While many African states draw on overlapping international, AU, and REC normative influences, comparative scholarship shows that these shared reference points do not yield uniform national laws in design or implementation.⁶⁸ Scholars focused on African data protection also link divergent approaches to differences in legal and constitutional traditions and to the varied institutional and economic contexts within which data governance regimes develop.⁶⁹ This diversity emphasizes the limitations of uniform, model-law approaches and cautions against assuming either inevitable convergence or uniform fragmentation.⁷⁰ Rather, it supports analytical frameworks that can handle variations without assuming convergence or fragmentation.⁷¹

Overall, the literature focused on Africa suggests that CBDF governance on the continent results from a complex mix of continental integration objectives (including the AfCFTA’s emerging digital trade framework), persistent cross-jurisdictional diversity in domestic legal design, and uneven implementation capacity.⁷² These insights shape the analytical approach taken in this thesis and lay the groundwork for evaluating the connection between continental CBDF commitments and local legal systems without assuming uniformity or dysfunction as a baseline.

⁶⁷ See Brian Daigle, “Data Protection Laws in Africa: A Pan- African Survey and Noted Trends” (2021) *Journal of International Commerce and Economics* 1–27 at 7–9; See also Graham Greenleaf & Bertil Cottier, “International and regional commitments in African data privacy laws: A comparative analysis” (2022) 44 *Computer Law & Security Review* 105638.

⁶⁸ See: Greenleaf & Cottier, “Comparing African Data Privacy Laws”, *supra* note 57 at 4; Also, see generally: Greenleaf & Cottier, “International and regional commitments in African data privacy laws”, *supra* note 67.

⁶⁹ See: *Regulating Data Protection and Cybersecurity in Africa: Findings from the Global Data Regulation Diagnostic*, by World Bank Group, in *Governance and the Digital Economy in Africa Technical Background Paper Series* (Washington, DC.: World Bank Group, 2023) at 28 online: <<https://openknowledge.worldbank.org/server/api/core/bitstreams/62e27761-1da1-467f-99a2-a6a1a3cf3b54/content>>; See: Justin Bryant, “Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights” at 430.

⁷⁰ See Mercy King’ori, “Cross-Border Data Flows in Africa: Examining Policy Approaches and Pathways to Regulatory Interoperability” (2024) June Issue *Future of Privacy Forum*, online: <<https://fpf.org/wp-content/uploads/2025/06/June-Issue-Brief-Cross-Border-Data-Flows-in-Africa.pdf>> at 4.

⁷¹ See generally: Alex B Makulilo, “Myth and reality of harmonisation of data privacy policies in Africa” (2015) 31:1 *Computer Law & Security Review* 78–89.

⁷² Vásquez Callo-Müller & Sucker, “Evolving approaches to cross-border data flows”, *supra* note 59 at 8.

2.3 Limitations in Existing Scholarship

The literature reviewed in the previous sections provides a detailed account of how cross-border data flows (CBDF) are understood in digital trade law, how regulatory diversity is discussed, and how African data governance fits into broader integration debates. However, these areas of study have some shortcomings that limit their ability to support systematic evaluations of how continental trade commitments interact with domestic CBDF systems.

One limitation in the trade-law scholarship on cross-border data flows is that it often operates at a high level of abstraction, organized around competing regulatory models and normative trade-offs. Much of the trade-law literature emphasizes general legal frameworks, classifications, and debates, such as the free flow of data with exceptions, regulation based on sovereignty, or rights-based approaches, rather than offering replicable analytical tools for evaluating specific domestic legal systems against regulatory benchmarks derived from trade-law and data-governance commitments. Although this scholarship is essential for understanding the development of CBDF rules, it provides little direction on how to assess the alignment or interaction across various legal systems in practice.

Another limitation arises from the frequent dependence on prescriptive models of regulatory coordination.⁷³ Such models often assume that regulatory alignment is both desirable and attainable, even where political, institutional, and administrative conditions make this unlikely. In Africa, this tendency may obscure the legal and administrative differences that define domestic data governance systems. It can lead to analyses that measure national laws against unrealistic standards instead of examining how regulatory systems operate within their own contexts.

⁷³ For example, Aaronson critiques prescriptive global models that assume convergence without regard to domestic governance realities. See Aaronson, *supra* note 5 at 6–9.

Lastly, current approaches generally treat continental and domestic frameworks as separate, rather than exploring their interaction. Trade-law reviews of continental instruments often do not closely examine domestic CBDF systems, while studies at the country level usually note regional commitments only briefly. This separation reduces the literature's ability to assess how continental digital trade rules are received, adjusted, or challenged within domestic legal frameworks.

Together, these limitations highlight the need for an evaluation method that acknowledges legal diversity, institutional context, and implementation practices, without assuming convergence or dysfunction. Rather than aiming to replace existing scholarship, the analytical framework developed in the next section aims to build on these works by providing a structured way to analyze how continental CBDF commitments and domestic legal systems relate to each other in practice.

2.4 Analytical Framework for Assessing AfCFTA CBDF Alignment

The previous sections have shown that current research on cross-border data flows (CBDF) offers valuable insights but a limited way to examine how continental trade commitments interact with domestic laws in practice. The literature generally works at either a very abstract level or remains confined to specific doctrines or policies. This limits its ability to support thorough, comparative evaluations. Given this situation, this section presents the analytical framework used in this thesis to assess the relationship between AfCFTA CBDF commitments and domestic regulatory systems. The framework does not aim to create a new theory of data governance or suggest an ideal regulatory model. Instead, it serves as a tool for evaluation. It organizes insights from trade law, data protection law, and regional integration studies to enable structured comparisons. It aims to help analyze how domestic CBDF regimes relate to continental trade commitments while considering legal diversity, institutional context, and implementation practices.

The framework is intentionally narrow in focus. It does not aim to measure the economic impact of cross-border data flows, evaluate regulatory efficiency, or predict how CBDF alignment affects trade volumes, investment, or digital market growth. It also does not assess the desirability of specific regulatory models. Its focus is strictly on the legal, institutional, and governance relationships between continental CBDF commitments and domestic regulatory regimes, as well as the conditions under which this alignment can be measured in legal and regulatory terms.

The framework consists of five analytical dimensions, each based on themes identified in the literature reviewed in Sections 2.2 and 2.3. Together, these dimensions encapsulate the key legal, institutional, and contextual factors that influence CBDF governance in the context of trade integration.

2.4.1 Legal-Normative Foundations

This dimension explores the legal basis and principles behind CBDF regulation. It looks at how data flows are understood within trade and data governance frameworks, including the essential obligations and allowable public policy exceptions. Drawing from trade law scholarship, it assesses whether domestic regimes reflect regulatory approaches that align with the AfCFTA's digital trade goals without assuming that all legal designs are the same.

2.4.2 Substantive Regulatory Scope

This dimension examines the actual content of CBDF rules, including the types of data involved, conditions for cross-border transfers, and whether data localization requirements exist. It allows for comparisons of how domestic laws manage data movement in practice and whether these frameworks effectively align with continental commitments. The focus is on regulatory methods rather than outcomes.

2.4.3 Institutional and Implementation Mechanisms

Acknowledging the limits of relying solely on text, this dimension emphasizes governance structures and enforcement protocols. It investigates which institutions oversee CBDF regulation, how power is distributed, and how compliance is monitored and enforced. This dimension highlights how institutional capacity and administrative setups influence the practical application of CBDF rules.

2.4.4 Rights and Digital Safeguards

This dimension looks at how individual and collective interests affected by cross-border data flows are protected, including privacy rights, data security, and access to remedies. Influenced by research that emphasizes trust and legitimacy in digital trade, it evaluates whether domestic CBDF regimes have safeguards that support cross-border data movement without compromising fundamental protections.

2.4.5 Socio-Economic and Technical Context

This dimension examines the broader context of CBDF regulation. It considers factors such as digital infrastructure, market development, and technical capability, which are recognized in the literature as crucial for effectively implementing CBDF commitments. Instead of viewing these conditions as outside influences, the framework treats them as essential for understanding regulatory alignment in practice.

Together, these five dimensions aim to capture the main variables identified in the literature that affect CBDF governance in a trade integration context. Legal-normative foundations and substantive regulatory scope concern the design of CBDF rules; institutional and implementation mechanisms along with rights and digital safeguards relate to governance and legitimacy; and socio-economic and technical context situates legal alignment within facilitating conditions. Other

relevant considerations, like sector-specific regulations or broader geopolitical factors, are not treated as separate dimensions, as they are included within these categories or lie outside the evaluative scope of this thesis.

Collectively, these five dimensions provide a structured way to examine how domestic CBDF regimes interact with AfCFTA digital trade commitments across legal, institutional, and contextual aspects. The framework does not assume convergence, fragmentation, or regulatory success. Instead, it enables comparative assessments by identifying areas of compatibility, tension, and divergence, which will be analyzed in the following chapters.

The next section describes how this framework is put into action for comparative analysis, using qualitative indicators and heuristic scaling to support systematic evaluation without oversimplifying complex legal issues into mere quantitative measures.

2.5 Operationalization of the Framework

The goal of this framework is not to measure legal compliance or produce empirical data but to offer a clear and systematic way to evaluate how well AfCFTA CBDF commitments match up with domestic regulatory systems across five analytical dimensions or *vice versa*.

The framework uses a qualitative comparative approach. Each dimension is evaluated using specific indicators drawn from legal texts, institutional setups, and documented regulatory practices. These indicators help organize the analysis and ensure consistency across case studies, rather than generating statistically comparable results. The focus remains on legal reasoning, doctrinal interpretation, and institutional assessment, in line with the methodology discussed in Chapter 1.

To clarify comparisons, the framework employs simple ordinal scales to show levels of alignment within each dimension. These scales function as interpretive tools to help synthesize complex legal and institutional information. They are not meant to be precise measurements of regulatory performance. Each scale represents a range of alignment—from low to high—based on how much domestic systems exhibit features that match AfCFTA CBDF commitments in design, scope, and implementation. Importantly, using ordinal scaling does not suggest that alignment is a linear process or can be reduced to numerical values; it simply aids in structured comparisons across jurisdictions.

This process unfolds in three steps. First, relevant legal documents, regulations, and policy statements are identified for each jurisdiction, paying attention to both binding rules and authoritative guidance. Second, these materials are analyzed against the indicators linked to each analytical dimension, focusing on how CBDF rules are defined, managed, and enforced in practice. Third, qualitative judgments are made about the degree of alignment observed, backed by doctrinal analysis, institutional evidence, and, when relevant, examples of enforcement or implementation. To address concerns about bias, the framework includes clear coding criteria for each dimension, consistently applied across all case studies. These criteria define the legal and institutional features that are relevant to alignment assessments and are presented transparently for critical review. While some judgment is inevitable in the qualitative legal analysis, this structured approach aims to limit discretion and improve analytical clarity.

Detailed indicators, coding criteria, and sample alignment scales are included in Appendix A. Their placement outside the main text is intentional, allowing for a focused analysis while maintaining transparency. This ensures that the comparative study is clear and replicable, without overshadowing the legal analysis central to the thesis.

Through this process, the framework allows a systematic look at how domestic CBDF systems relate to AfCFTA digital trade commitments across different dimensions, while respecting the boundaries of doctrinal and institutional legal analysis. The framework is utilized in Chapter 4 for the comparative assessment of Nigeria, Kenya, and South Africa, and its implications for continental digital trade integration are explored in the following chapters.

2.6 Conclusion

This chapter has reviewed the main bodies of research relevant to cross-border data flows (CBDF) in the context of digital trade and regional integration. It focuses on legal approaches to data flows in trade agreements, discussions about regulatory diversity and coordination, and analyses of data governance in Africa. The review shows that while the literature offers important conceptual and contextual insights, it often operates at a level of abstraction or fragmentation that hinders a systematic evaluation of how continental trade commitments interact with domestic CBDF regimes.

To address these limitations, the chapter has developed an analytical framework aimed at facilitating a structured assessment of how AfCFTA CBDF commitments align with domestic regulatory regimes. This framework builds on existing research and is explicitly evaluative rather than prescriptive. Its five dimensions—legal-normative foundations, substantive regulatory scope, institutional and implementation mechanisms, rights and digital safeguards, and socio-economic and technical context—reflect the key factors identified in the literature that shape CBDF governance within trade integration.

The chapter also details how this framework is applied through qualitative indicators and heuristic scaling, with clear coding criteria to ensure analytical coherence and transparency. This approach

allows for comparative analysis without oversimplifying complex legal and institutional issues into quantitative metrics or assuming that regulatory convergence is the goal.

Together, the literature review, analytical framework, and implementation outlined in this chapter lay the methodological groundwork for the rest of the thesis. The next chapter builds on this foundation by examining the AfCFTA Digital Trade Protocol and its CBDF-related provisions as a continental legal benchmark against which domestic regulatory regimes will be later assessed.

Chapter 3: Legal Architecture of CBDF Under the AfCFTA Digital Trade Protocol and its CBDF Annex

3.1 Introduction

In this chapter, the AfCFTA Digital Trade Protocol and the CBDF Annex are examined as a legal reference. The goal is to clarify the rules, main principles, safeguards, and institutional setups that govern CBDF under the AfCFTA. This will provide a clear point of reference for later comparisons.

It is important to mention at this juncture that examining the AfCFTA CBDF system as a benchmark does imply that this thesis assumes it is the best or most settled regulatory model. Also, this chapter does not evaluate the effectiveness of the Protocol or predict its economic or developmental effects as that is outside the scope of this thesis. Instead, using the AfCFTA as the benchmark serves as a way to interpret the legal reasoning and design aspects of the AfCFTA's approach to CBDF. It will help examine how domestic regulations compare in terms of alignment, tension, or difference. This method reflects the evaluative approach detailed in the previous Chapter and does not assume regulatory success or convergence.

This chapter is divided into seven sections. Section 3.2 explains the legal status and scope of the Digital Trade Protocol and its Annexes within the AfCFTA framework. Section 3.3 explores the foundational norms of CBDF governance under the AfCFTA, highlighting the balance between trade facilitation and regulatory independence. Section 3.4 outlines the main rules governing cross-border data flows. Section 3.5 discusses the exceptions, safeguards, and regulatory independence structures. Section 3.6 reviews the institutional framework and implementation arrangements envisaged for CBDF governance. Section 3.7 brings these elements together to define the AfCFTA

CBDF benchmark. Finally, Section 3.8 concludes by explaining how this benchmark will aid in evaluating domestic CBDF systems in the next chapter.

3.2 Legal Status and Scope

The AfCFTA Digital Trade Protocol is part of the legal framework of the African Continental Free Trade Area.⁷⁴ It works alongside the AfCFTA Agreement and its other Protocols. Adopted under the AfCFTA framework, the Digital Trade Protocol serves as a binding treaty for State Parties that have ratified it. This is subject to the general rules of the AfCFTA regarding entry into force, implementation, and interpretation. Its legal status distinguishes it from non-binding policy tools or model laws and positions it firmly within the AfCFTA treaty system.⁷⁵

The Digital Trade Protocol serves as a framework instrument that includes Annexes for specific regulatory areas.⁷⁶ The Protocol states that its Annexes are an essential part of the treaty and elaborate on its general commitments and objectives.⁷⁷ The Annex on Cross-Border Data Flows (CBDF Annex) is intended to outline specific rules related to the transfer of data across borders while working alongside the Protocol's main principles and scope.⁷⁸ Therefore, the CBDF Annex should not be read alone; it must be understood in the context of the entire Protocol.

⁷⁴ See *AfCFTA Digital Trade Protocol*, *supra* note 13 at Article 2.

⁷⁵ See African Union, *supra* note 10 at 15–18.

⁷⁶ The Protocol creates 8 Annexes in Article 46. For a summary of what the annexes are about, see generally: Tralac, “Summary of the Annexes to the AfCFTA Protocol on Digital Trade”, online (<https://www.tralac.org/documents/events/tralac/5918-2025-conference-two-pager-summary-of-the-annexes-to-the-afcfta-protocol-on-digital-trade/file.html>): *2025 Tralac Annual Conference*.

⁷⁷ *AfCFTA Digital Trade Protocol*, *supra* note 13 at Article 46.

⁷⁸ *Ibid* at Article 20; *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 at Article 2.

Regarding scope, the Digital Trade Protocol applies to digital trade activities within the AfCFTA framework, subject to the limitations and exclusions stated in the Protocol and its Annexes.⁷⁹ While the Protocol does not aim to create a complete system for managing all aspects of data governance, such as data collection, storage, or domestic processing, it still influences these areas as long as national measures impact digital trade or limit cross-border data transfers. Broader areas of data protection, cybersecurity, and digital regulation remain governed by domestic legal systems, but within the constraints imposed by AfCFTA trade obligations, particularly where such measures have the effect of limiting cross-border data flows. The Protocol's provisions are therefore primarily concerned with the trade-related dimensions of digital activity, including the conditions under which data may move across borders for commercial purposes.

The CBDF Annex specifically addresses cross-border data transfers related to digital trade. Its scope is defined by the movement of data across national borders, rather than the entire process of data management within a country. Thus, domestic laws still oversee data collection, storage, and use within national areas, depending on how those laws interact with the AfCFTA's trade-related commitments.

Lastly, the legal status and scope of the Digital Trade Protocol should be viewed within the broader institutional context of the AfCFTA. This context emphasizes gradual implementation, cooperation, and regulatory flexibility among State Parties with varying legal and administrative capacities. This setting influences both the design and expected function of CBDF rules under the AfCFTA. It reinforces the view of the Protocol and its Annexes as legal standards for analysis rather than a fully unified or self-operating system for data governance.

⁷⁹ This include government procurement and government data. See: *AfCFTA Digital Trade Protocol*, *supra* note 13 at Article 3.; It also excludes non-digital trade data. See: *Annex on Cross-Border Data Transfers*, *supra* note 78 at Article 3.

3.3 Normative Foundations of CBDF under the AfCFTA Digital Trade Protocol

The AfCFTA Digital Trade Protocol addresses cross-border data flows (CBDF) using a logical approach. It aims to support digital trade while maintaining the ability of governments to regulate for important public policy goals. This approach seeks a balance in trade law by enabling market integration and reducing unnecessary barriers. It acknowledges that data governance involves interests like privacy, security, and public order that need regulatory protection. Therefore, the Protocol does not see CBDF liberalization as an end goal. Instead, it views it as a conditional commitment included within a broader system of safeguards and flexibility.

At the heart of this approach is the understanding that data flows are an important part of digital trade, not just a separate regulatory issue. The Protocol's goals and principles prioritize trade facilitation, cooperation, and integration in the digital economy. It positions CBDF rules within a practical trade context. This perspective differentiates the AfCFTA approach from more comprehensive data governance frameworks. It indicates that CBDF commitments aim to reduce trade-related barriers rather than replace national control over data protection and cybersecurity.

This framework aligns with broader trends in modern digital trade agreements. Typically, these agreements combine commitments to support cross-border data flows with clear protections for privacy, security, and other public policy goals. Academic insights suggest that such agreements rarely pursue unrestricted data movement; instead, they seek to balance trade liberalization with the need for regulatory legitimacy in sensitive areas. Agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA) follow this "facilitation with exceptions" approach. They embed rules for data flows within a structure that maintains national regulatory authority. This trend

indicates that the AfCFTA's stance is part of a common trade-law pattern rather than an unusual or overly restrictive strategy.

The Protocol also acknowledges the regulatory differences among State Parties and incorporates this recognition into its framework. Rather than enforcing a single regulatory model, the AfCFTA structure allows for variations in domestic laws by linking CBDF facilitation with room for public policy regulation. This method aligns with trade law practices that handle regulatory diversity through conditional rules and exceptions, rather than enforcing uniform standards. The focus on cooperation and gradual implementation shows an awareness of the varying levels of institutional capacity and digital development across the continent.

A key aspect of the AfCFTA's framework is how it presents CBDF commitments alongside protections for privacy, security, and other valid objectives. The structure suggests that trust in cross-border data movement is not taken for granted but must be built through sound regulatory practices. By incorporating safeguards into the framework rather than treating them as external limits, the AfCFTA acknowledges that successful digital trade relies on the credibility of domestic regulatory systems as much as on the formal openness of data flows.

This balance is further strengthened by the Protocol's preference for flexibility in legal methods. Open standards, cooperation provisions, and references to national regulatory goals indicate a desire to handle CBDF governance through collaboration instead of strict obligations. These strategies align with trade instruments that deal with sensitive regulatory areas, where legal certainty is important but should respect national regulatory choices.

In summary, the normative basis of CBDF under the AfCFTA can be seen as supportive but with conditions. The Protocol promotes digital trade integration by recognizing the significance of cross-border data flows while maintaining regulatory autonomy through safeguards, flexibility,

and cooperation among institutions. This framework sets the stage for understanding and interpreting the specific CBDF rules that follow.

3.4 Substantive Disciplines Governing CBDF

This section examines the key legal rules surrounding cross-border data flows (CBDF) under the AfCFTA Digital Trade Protocol and its Annex on Cross-Border Data Transfers. These rules put into action the balance discussed in Section 3.3 by clarifying when cross-border data transfers are allowed, how restrictive regulations are controlled, and under what conditions limits may be set. Together, they lay out the main legal framework of the AfCFTA CBDF benchmark.

3.4.1 Cross-Border Data Transfer Obligations and Scope

The main CBDF requirement is found in Article 20(1) of the Digital Trade Protocol.⁸⁰ It mandates that State Parties, subject to the CBDF Annex, must allow the cross-border transfer of data, including personal data, electronically for digital trade conducted by individuals from a State Party.⁸¹ This rule makes cross-border data transfers generally allowed in the AfCFTA digital market and connects the obligation to the Annex for its detailed guidelines and restrictions.

The CBDF Annex supports this obligation by generally prohibiting State Parties from implementing or keeping measures that limit cross-border data transfers for digital trade.⁸² These measures include various restrictions found in laws, regulations, and administrative practices, whether they are temporary or permanent.⁸³ This approach ensures that both official legal barriers and real-world administrative challenges are covered by the CBDF rules.

⁸⁰ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 20(1).

⁸¹ *Ibid.*

⁸² *Annex on Cross-Border Data Transfers*, *supra* note 78 art 16(1).

⁸³ *AfCFTA Digital Trade Protocol*, *supra* note 13 at 1(n).

At the same time, the Protocol and Annex limit CBDF obligations to transfers made for digital trade. Transfers unrelated to digital trade, as well as data held or processed by a State Party in a governmental role, are not covered by the CBDF rules.⁸⁴ This focus reinforces that the AfCFTA CBDF rules are trade regulations rather than complete data governance norms, while also keeping domestic authority over internal data processing.

Importantly, neither the Digital Trade Protocol nor the Annex on Cross-Border Data Transfers prescribes a particular legislative form for domestic data protection regimes. The AfCFTA CBDF framework is regulatory-form neutral, permitting State Parties to rely on comprehensive data protection statutes, sector-specific regulatory regimes, or hybrid models, provided that the resulting domestic framework delivers functionally equivalent safeguards and enables cross-border data transfers consistent with the Protocol's objectives. This form-neutral approach reflects the AfCFTA's emphasis on regulatory interoperability and cooperation rather than formal harmonisation and accommodates the diverse institutional capacities and regulatory traditions of State Parties.

3.4.2 Data Localisation and Computing Facilities Requirements

Alongside data transfer obligations, the Digital Trade Protocol regulates data localisation measures through Article 22.⁸⁵ This article stops State Parties from requiring individuals from another State Party to use or place computing facilities within their borders as a requirement for engaging in digital trade. Instead of addressing data localisation in vague terms, this provision focuses on a specific regulation, mandatory local infrastructure, that affects market access and digital trade integration.

⁸⁴ *Ibid* art 3(2)(a); *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade*, *supra* note 13 art 3(1).

⁸⁵ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 22(1).

However, the prohibition is not absolute. Article 22 allows State Parties to enact measures that run counter to this obligation when necessary to meet important public policy goals or protect essential security interests, provided those measures are applied fairly and are no more restrictive than necessary.⁸⁶ Notably, the Annex does not contain any explicit or standalone provision on data localisation. Thus, the AfCFTA CBDF benchmark recognizes localization as a regulated policy tool, whose acceptability relies on justification and fairness, not as an automatically illegal measure.

3.4.3 Non-Discrimination, Equivalence, and Transfer Conditions

The CBDF framework also includes standards designed to prevent biased or protective treatment in regulating data flows. The Annex requires that State Parties provide no less favorable treatment to data, including personal data, from individuals of other State Parties than to similar data from domestic individuals or third parties.⁸⁷ This ensures CBDF governance aligns with established trade law principles of equal treatment and neutrality.

Additionally, the Annex requires that data transferred from another State Party receive the same level of protection as domestic data.⁸⁸ However, this does not require identical data protection laws across different regions. Instead, it sets a standard that allows for regulatory differences while ensuring that cross-border transfers do not lower protection simply due to the data's origin.

These rules are backed by legal standards that guide regulatory discretion. Restrictions on cross-border data transfers need to be justified by legitimate purposes and must be applied fairly and proportionately.⁸⁹ By using these methods, the AfCFTA CBDF system breaks down trade-restrictive measures without enforcing a single regulatory approach.

⁸⁶ *Ibid* art 22(2).

⁸⁷ *Annex on Cross-Border Data Transfers*, *supra* note 78 art 18(1).

⁸⁸ *Ibid* art 18(2).

⁸⁹ *Ibid* arts 18 & 24.

3.4.4 Transfer Mechanisms and Regulatory Cooperation

Understanding that facilitating CBDF relies on effective ways to safely move data, the Annex encourages State Parties to support and recognize various cross-border data transfer mechanisms.⁹⁰ These can include certification systems,⁹¹ regional data centers,⁹² cloud computing infrastructure, sector-specific codes of conduct,⁹³ and other accepted safeguards, as long as they meet applicable data protection standards and do not create unnecessary administrative hurdles.⁹⁴

This focus on mechanisms and cooperation reflects a governance model aimed at interoperability rather than centralized control. By favoring mutual recognition, standards-based strategies, and regulatory collaboration, the AfCFTA CBDF framework aims to enable practical data flows while accommodating diverse domestic regulatory systems. These provisions are essential to the substantive benchmark, indicating that coordination is to be achieved through aligned regulatory practices rather than uniform legal rules alone.

3.4.5 The AfCFTA CBDF Benchmark

Altogether, the substantive CBDF rules under the AfCFTA create a benchmark defined by conditional facilitation, regulatory equality, and cooperation-focused governance. Cross-border data transfers are generally allowed for digital trade purposes, localization requirements are regulated without outright banning them, and regulatory diversity is managed through non-discrimination, equivalence, and justified conditions. This benchmark serves as the legal reference point against which domestic CBDF systems are evaluated in Chapter 4 and through which potential alignments are considered in Chapter 5.

⁹⁰ *Ibid* art 19.

⁹¹ *Ibid* art 19(1)(d).

⁹² *Ibid* art 19(1)(a).

⁹³ *Ibid* at 19(4)(c).

⁹⁴ *Ibid* art 19(4).

3.5 Exceptions, Safeguards and Regulatory Autonomy

The cross-border data transfer commitment in the Digital Trade Protocol and the CBDF Annex exist within a system of exceptions and safeguards, framed as legitimate public policy. This legitimate public policy ensures regulatory independence affirming the right of state to regulate which is also explicitly captured in the Protocol.⁹⁵ These exceptions are core to the AfCFTA CBDF framework; they shape the conditions under which cross-border data flow obligations apply.

3.5.1 Public Policy and Essential Security Exceptions

Article 20(2) of the Digital Trade Protocol allows State Parties to adopt or maintain measures that conflict with the requirement for cross-border data transfers.⁹⁶ This is acceptable when those measures are needed to meet legitimate public policy goals or to protect essential security interests. Such measures must not result in arbitrary or unjustifiable discrimination or hidden trade restrictions.⁹⁷ This article creates a general exception that modifies the CBDF transfer obligation in Article 20(1).⁹⁸

A similar exception system applies to data localization rules. Article 22(2) of the Protocol permits deviations from the ban on requiring the use or location of computing facilities within a nation when justified by public policy goals or security concerns.⁹⁹ These also need to meet conditions of non-discrimination and necessity. The alignment between Articles 20 and 22 shows a unified approach to regulatory independence across the main CBDF disciplines.

⁹⁵ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 4 affirms the right of state parties to regulate.

⁹⁶ *Ibid* art 20(2).

⁹⁷ *Annex on Cross-Border Data Transfers*, *supra* note 78 art 23(2).

⁹⁸ {Citation}

⁹⁹ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 22(2).

Notably, the scope of the public policy exceptions recognized in the CBDF Annex is broad which appears to be deliberate. The Annex enumerates public policy objectives without defining them exhaustively, which introduces a degree of indeterminacy. However, this openness does not necessarily undermine regulatory discipline. The Protocol and Annex subject any reliance on public policy exceptions to necessity, proportionality, and non-discrimination requirements.¹⁰⁰ This shifts the analytical focus from the content of the policy objective to the manner in which it is designed and applied. In this sense, the exception framework does not function as a blanket carve-out, but as a conditional mechanism that preserves regulatory autonomy while constraining opportunistic or protectionist uses of data governance measures. This is consistent with the AfCFTA's broader approach to digital trade integration, which prioritizes managed regulatory diversity over rigid harmonization in light of varying domestic legal systems and institutional capacities.

3.5.2 Privacy, Data Protection, and Trust-Based Safeguards

Alongside public policy exceptions, the CBDF Annex includes specific safeguards focused on privacy and data protection. Article 17 of the Annex mandates that data transferred from another State Party should receive the same level of protection as domestic data.¹⁰¹ This requirement serves both as a standard and as a safeguard that influences the acceptability of cross-border data flows. Article 18 of the Annex reinforces this by prohibiting unfair treatment of data from another State Party.¹⁰² Together, these provisions establish trust-based safeguards in the CBDF framework. They ensure that facilitating data flows does not lead to weaker protection simply due to the cross-border transfer.

¹⁰⁰ *Annex on Cross-Border Data Transfers*, *supra* note 78 art 23.

¹⁰¹ *Ibid* art 17.

¹⁰² *Ibid* art 18.

3.5.3 Institutional Safeguards and Cooperative Mechanisms

The AfCFTA CBDF framework's regulatory independence is further backed by cooperation-oriented institutional setups. The Digital Trade Protocol highlights cooperation, dialogue, and sharing information among State Parties in applying digital trade rules. Article 19 of the CBDF Annex encourages the use and recognition of a variety of transfer methods like certification schemes, codes of conduct, and regional data infrastructure, as long as these methods promote secure and lawful data transfers.¹⁰³ These cooperative mechanisms ease the application of CBDF obligations by favoring coordination over centralized enforcement. They also recognize different regulatory capacities among State Parties.

3.5.4 Implications for the AfCFTA CBDF Benchmark

Overall, the exceptions, safeguards, and cooperation practices found in the Digital Trade Protocol and CBDF Annex create a benchmark for CBDF that emphasizes conditional openness and structured regulatory independence. Cross-border data flows are generally allowed but remain under clear legal limits grounded in public policy, security, and data protection needs which must be applied only as necessary and in a non-discriminatory manner. This summarizes the AfCFTA CBDF benchmark and provides the legal framework for assessing domestic CBDF regimes in Chapter 4.

3.6 Institutional Framework and Implementation Arrangements

The operation of the AfCFTA CBDF regime is shaped by both substantive obligations and exceptions, as well as by the institutional framework and implementation arrangements set up under the AfCFTA Establishment Agreement and the Digital Trade Protocol. These arrangements

¹⁰³ *Ibid* art 19.

provide the governance context for interpreting, coordinating, and gradually implementing CBDF commitments. Instead of creating a separate enforcement system for data flows, the Protocol incorporates CBDF governance within the broader AfCFTA institutional framework, highlighting cooperation, dialogue, and flexibility.

3.6.1 Institutional Placement within the AfCFTA Framework

The Digital Trade Protocol is carried out through the existing structures of the AfCFTA, including the AfCFTA Secretariat and relevant committees established under the Agreement and its Protocols. The Protocol expects that issues related to digital trade, including CBDF, will be managed by designated institutional bodies responsible for monitoring implementation, facilitating cooperation, and tackling implementation challenges. This positioning places CBDF governance within a multilateral, committee-based trade governance model rather than a separate regulatory authority.

By incorporating CBDF oversight within AfCFTA institutions, the Protocol promotes coherence with other trade rules while enabling coordination across related policy areas. This approach favors integration and coordination instead of forming separate enforcement bodies for digital trade.

The AfCFTA Digital Trade Protocol is designed to be implemented through the AfCFTA institutional framework, rather than a new standalone regulator. The AfCFTA Agreement establishes an implementation structure that includes the Council of Ministers, the Committee of Senior Trade Officials, and the AfCFTA Secretariat for implementation, administration, facilitation, monitoring, and evaluation.¹⁰⁴ The Council of Ministers consists of the Ministers for trade or other designated authorities of State Parties. Article 11 of the Agreement empowers the Council with the authority to create and delegate tasks to committees and working groups.¹⁰⁵

¹⁰⁴ *AfCFTA Establishment Agreement*, *supra* note 27 art 9.

¹⁰⁵ *Ibid* art 11(3)(f).

Building on this setup, the Digital Trade Protocol establishes a specialized Committee on Digital Trade as part of AfCFTA institutional architecture.¹⁰⁶ This committee will implement the Protocol and pursue its goals, which may involve sub-committees and working groups as needed. The Protocol also gives the Committee on Digital Trade the responsibility for monitoring and evaluation.¹⁰⁷ Reports will go to the Council of Ministers through the Committee of Senior Trade Officials.¹⁰⁸ The Secretariat is expected to support this monitoring role and prepare annual implementation reports.¹⁰⁹

In this governance model, oversight of cross-border data transfer (CBDF) is seen as part of a unified AfCFTA implementation system. This committee-based approach aligns with policy analysis that describe the Protocol as a digital trade framework for AfCFTA.¹¹⁰ It focuses on coordinated trade rules, regulatory cooperation, and implementation led by institutions. It does not involve the establishment of a separate digital regulator.

3.6.2 Cooperation and Information Exchange

A key aspect of the institutional design is the focus on cooperation and information exchange among State Parties. The Digital Trade Protocol encourages States to work together on digital trade implementation matters, including regulatory approaches, best practices, and capacity building. In the CBDF Annex, Article 19 supports this focus by urging cooperation in developing and recognizing cross-border data transfer mechanisms and safeguards.

These cooperation and information-exchange provisions create procedural and coordination duties instead of direct enforcement responsibilities. Their goal is to facilitate dialogue, mutual learning,

¹⁰⁶ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade*, *supra* note 13 art 37.

¹⁰⁷ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 49.

¹⁰⁸ *Ibid* art 49(1).

¹⁰⁹ *Ibid* art 49(2).

¹¹⁰ See generally: Kholofelo Kugler, *supra* note 24; Alberto Lemma & Prachi Agarwal, “Implementing the Digital Trade Protocol of the African Continental Free Trade Area” ODI.

and gradual convergence in regulatory practices, rather than to impose uniform legal rules or immediate compliance outcomes.

3.6.3 Relationship to Dispute Settlement

The Digital Trade Protocol does not set up a specific dispute settlement mechanism for CBDF. Instead, disputes related to CBDF obligations fall under the AfCFTA's general dispute settlement framework.¹¹¹ This choice reinforces the integration of CBDF governance within the broader AfCFTA legal framework and avoids treating data flows as a separate type of trade dispute.

The lack of a specific enforcement or fast-tracked dispute resolution process for CBDF could also highlight the AfCFTA's preference for cooperative governance in this area. It positions formal dispute resolution as a secondary, rather than primary, option for addressing CBDF-related tensions.

3.6.4 Implications for the AfCFTA CBDF Benchmark

The institutional and implementation arrangements under the Digital Trade Protocol complete the AfCFTA CBDF benchmark by clarifying how substantive obligations and exceptions are meant to function in practice. CBDF governance is characterized by integration within AfCFTA institutions, reliance on cooperation and information exchange, and accommodation of regulatory diversity through progressive implementation.

As a result, the institutional design strengthens the AfCFTA CBDF regime as a flexible benchmark for evaluating regulatory alignment over time, rather than as a compliance-driven framework imposing immediate or uniform implementation requirements.

¹¹¹ *AfCFTA Digital Trade Protocol*, *supra* note 13 art 45.

3.7 Synthesis of the AfCFTA CBDF Benchmark

The provisions discussed in Sections 3.2 through 3.6 establish a standard that highlights a unique approach to CBDF governance. This approach prioritizes facilitation, demands openness based on regulatory legitimacy, and manages diversity through organized flexibility and cooperation.

On a normative level, the AfCFTA CBDF system is based on a supportive but limited view of data mobility. Cross-border data flows are seen as essential for digital trade integration, but they are not viewed as absolute or independent rights. Instead, CBDF obligations are part of a framework that maintains regulatory authority for valid public policy goals. These goals include privacy protection and important security interests. This balance frames data mobility as a tool for trade integration rather than a goal in itself.

In terms of substance, this standard focuses on conditional rules rather than absolute regulations. The requirement to allow cross-border data transfers for digital trade exists alongside specific limitations. These include restrictions on the functional scope, rules on data localization through computing facility requirements, and fairness standards like non-discrimination and equivalence. These methods regulate trade-restrictive measures without requiring uniform regulatory frameworks, allowing for diverse regulations among State Parties.

The structure of exceptions further supports this conditional openness. Public policy and security exceptions, along with necessity and proportionality criteria, outline the legal limits of CBDF liberalization. Privacy and trust safeguards included in the Annex make sure that the facilitation of data flows is tied to credible protection standards rather than being pursued independently.¹¹² This means that regulatory autonomy is not only maintained but also shaped by legal conditions that connect domestic regulation with trade goals.

¹¹² *Annex on Cross-Border Data Transfers*, *supra* note 78 art 19(4) & 22.

Institutionally, the AfCFTA CBDF system focuses on cooperative governance rather than strict enforcement. CBDF commitments are carried out through existing AfCFTA bodies, emphasizing dialogue, information sharing, and gradual implementation. The lack of specific enforcement mechanisms for CBDF highlights the importance of coordination and regulatory learning as the primary means of ensuring alignment over time. Formal dispute resolution exists only as a backup. For analysis, this standard operates across four connected areas: (i) the legal and normative foundations of CBDF governance in the AfCFTA; (ii) the scope and design of CBDF rules, including data transfer obligations, localization rules, and fairness standards; (iii) the setup and function of exceptions and safeguards for regulatory autonomy; and (iv) the institutional and cooperative methods for implementing CBDF commitments at the continental level. These areas offer a structure for evaluating consistency and differences in domestic CBDF systems in the next chapter.

This standard does not measure the effectiveness, enforcement results, or economic consequences of CBDF regulations in real life. Instead, it serves as a legal and institutional reference point for assessing how domestic CBDF systems align with the AfCFTA framework.

This standard provides the analytical basis for the comparative analysis in Chapter 4. The next chapter applies the AfCFTA CBDF standard to the domestic regulatory systems in Nigeria, Kenya, and South Africa, exploring how national CBDF structures interact with or differ from the continental legal framework established by the AfCFTA.

Chapter 4: Domestic CBDF Regimes in Nigeria, Kenya, and South Africa

4.1.0 Introduction

This chapter uses the framework established in Chapter 2 to examine the domestic legal systems that control cross-border data flows (CBDF) in Nigeria, Kenya, and South Africa. It builds on the AfCFTA Digital Trade Protocol and the Annex on Cross-Border Data Transfers discussed in Chapter 3. The chapter looks at how national CBDF systems interact with, support, or limit the implementation of AfCFTA's commitments on digital trade and data movement. Domestic legal systems are seen as essential sites for putting AfCFTA CBDF obligations into practice, rather than as separate regulatory frameworks.

The chapter proceeds from ideas mentioned in Chapters 1 and 3. AfCFTA's CBDF framework relies on effective implementation. The Protocol and Annex outline binding obligations to allow cross-border data transfers for digital trade, bar unjustified data localization, and encourage regulatory cooperation. However, these commitments do not override domestic authority over data governance. They exist alongside national legal systems that vary in regulatory philosophy, institutional capacity, enforcement ability, and technical readiness. To assess alignment, we must go beyond mere textual comparisons and consider how domestic systems operate in practice within AfCFTA's trade law framework.

The analysis in this chapter focuses on diagnosis rather than providing solutions. Alignment is not the same as strict compliance, and misalignment is not viewed as a breach or illegal act. Instead, alignment refers to functional compatibility: how well domestic CBDF systems can support AfCFTA's trade goals without creating significant friction, uncertainty, or implementation delays. On the other hand, misalignment points to situations where domestic legal design, institutional practices, or contextual challenges significantly weaken the effectiveness or predictability of

AfCFTA's CBDF commitments. A domestic regime is considered compatible with the AfCFTA CBDF framework where its legal structure and administrative operation permit cross-border data transfers under predictable, transparent conditions that can be reconciled with AfCFTA obligations and safeguards. Compatibility in this sense does not require uniform transfer mechanisms or identical institutional models, but it does require that divergence does not operate as a de facto barrier to digital trade. This perspective acknowledges AfCFTA's recognition of regulatory independence, varying capacities, and valid public policy goals, as seen in the Protocol's right-to-regulate clause and the Annex's public interest safeguards.

Nigeria, Kenya, and South Africa are analyzed as comparative case studies because of their economic importance, regulatory development, and differing approaches to data governance in Africa's digital economy. Each country has a unique CBDF governance model influenced by distinct constitutional traditions, policy priorities, and market conditions. Together, they provide a broad view of how AfCFTA CBDF obligations interact with domestic systems in different African contexts, without suggesting that these examples cover all of the continent's regulatory diversity. To ensure consistency with the rest of the thesis, each country is analyzed using the five-dimension framework developed in Chapter 2. The analysis covers:

- i. The legal-normative basis of CBDF regulation.
- ii. The regulatory scope governing cross-border transfers, including transfer methods and data localization policies.
- iii. Institutional and implementation mechanisms, including enforcement power and regulatory cooperation.
- iv. Rights protections and digital safeguards for cross-border data processing.

- v. The socio-economic and technical context affecting the feasibility and implementation of CBDF rules.

These dimensions are applied in the same order across all three jurisdictions, making explicit reference to AfCFTA CBDF obligations, principles, and exceptions outlined in Chapter 3. Each section concludes with an assessment of AfCFTA CBDF alignment that summarizes findings across the five dimensions and identifies key sources of alignment or misalignment.

This chapter does not propose reforms or models for harmonization. Its goal is to present a fact-based account of how domestic CBDF systems currently interact with AfCFTA's legal framework, highlighting differences in doctrine, regulatory choices, institutional capacity issues, and contextual challenges. This diagnostic groundwork is critical for Chapter 5, which uses these comparative findings to explore ways to operationalize the AfCFTA CBDF regime while honoring regulatory diversity and varying implementation capacities among State Parties.

4.2.0 Nigeria

Nigeria is a key country for understanding how well it aligns with the AfCFTA cross-border data flow (CBDF) framework. As Africa's largest economy and a major digital market, Nigeria's approach to personal data governance affects not only local digital trade but also the ability of AfCFTA to facilitate smooth and consistent cross-border data transfers among member states. The country's CBDF rules are mainly outlined in the Nigeria Data Protection Act 2023 (NDPA) and regulations from the Nigeria Data Protection Commission (NDPC). The most important of these is the General Application and Implementation Directive 2025 (GAID), which creates the main framework for the cross-border transfer of personal data.

Nigeria's CBDF system allows cross-border data transfers but requires compliance with certain legal safeguards and regulatory oversight. This makes Nigeria a valuable case study for assessing how AfCFTA obligations connect with local systems that focus on data protection and regulatory control, without assuming complete openness or strict data localization.

In addition to this broad data protection framework, Nigeria's CBDF rules are influenced by specific regulations for certain sectors, such as finance and telecommunications, which add more conditions for data processing and transfer. These sector-specific regulations do not function as separate CBDF systems but interact with the NDPA's framework in ways that will be explored in the following sections.

Potential issues in Nigeria's CBDF system are less likely to arise from clear prohibitions on cross-border data transfers. Instead, they are often the result of multiple regulatory conditions, discretionary approval processes, and sector-specific limitations that dictate how transfers actually take place.

The significance of Nigeria as a case study lies in the complexity and strength of its domestic regulatory framework, rather than any formal differences from AfCFTA CBDF requirements. Nigeria has established a clear legal framework for cross-border transfers, including guidelines on adequacy, alternative transfer methods, and supervisory oversight. However, the actual implementation of these rules raises important questions about how domestic protections, regulatory discretion, and execution capacity interact with AfCFTA's goals of promoting cross-border digital trade. Thus, Nigeria serves as a crucial example of whether AfCFTA's commitments on data mobility can succeed in large digital economies with diverse regulatory environments, rather than through strict standardization.

Using the analytical framework from Chapter 2 and relevant references from Chapter 3, Nigeria's CBDF system will be analyzed across five related dimensions. First, the analysis will look at the legal and normative bases of Nigeria's CBDF system. Second, it will assess the regulatory scope surrounding cross-border transfers, including transfer methods and data localization risks. Third, it will evaluate the mechanisms for institutional and practical implementation, focusing on the powers and capacities of the NDPC. Fourth, it will review rights-based protections and digital safeguards related to cross-border data processing. Finally, it will consider Nigeria's CBDF system within its socio-economic and technical environment, exploring how infrastructure, market conditions, and regulatory capabilities impact the feasibility of implementing AfCFTA-aligned data mobility.

This five-dimensional evaluation will measure Nigeria's domestic CBDF framework against the guiding principles of the AfCFTA Digital Trade Protocol and the Annex on Cross-Border Data Transfers discussed in Chapter 3. Each section will examine whether Nigeria's legal arrangements and implementation conditions support or hinder AfCFTA's goals of regulatory cooperation, reliable data flows, and the protection of public policy interests. The Nigeria section will conclude with an alignment assessment of the AfCFTA CBDF, summarizing insights from all five dimensions.

4.2.1 Legal-Normative Foundations

Nigeria's legal framework for cross-border data flow (CBDF) governance is based on a rights-oriented approach that confirms significant regulatory power over how personal data is handled and moved. The Nigeria Data Protection Act 2023 (NDPA) designates data protection as essential for the Constitution, economy, and governance.¹¹³ It explicitly connects the protection of personal

¹¹³ See: *Nigeran Data Protection Act, 2023*, s 1(1).

data to Nigeria's role in regional and global digital economies while allowing the State to oversee data processing for public interest, security, and development goals.¹¹⁴ This dual focus is clear in the Act's goals, which seek to protect fundamental rights while also improving Nigeria's digital economy through responsible use of data.¹¹⁵

On a constitutional level, the NDPA puts into action the fundamental right to privacy found in section 37 of the 1999 Constitution. It turns informational privacy into a legally enforceable right instead of just a policy concern. The Act supports this rights-focused approach with mandatory guidelines for lawful, fair, and accountable data processing.¹¹⁶ It also enforces the rights of data subjects,¹¹⁷ and establishes a thorough system of regulatory oversight and remedies.¹¹⁸ This approach treats cross-border data governance as an extension of protecting constitutional rights, rather than merely a matter of trade facilitation.

Within this rights-based framework, Nigeria follows a conditional openness model for CBDF governance. Personal data transfers across borders are generally allowed but must comply with legal safeguards and regulatory requirements. Part VIII of the NDPA acknowledges cross-border data transfers while requiring that they meet adequacy determinations or alternative basis for transfer.¹¹⁹ This framework conceptually aligns with the AfCFTA Digital Trade Protocol, which accepts cross-border data flows as vital to digital trade while still allowing State Parties to regulate for legitimate public policy goals like privacy and security.

This conditional approach in Nigeria's CBDF structure is supported by a centralized regulatory philosophy in the NDPA. The Act creates the Nigeria Data Protection Commission (NDPC) as an

¹¹⁴ See: *ibid*, s 1(1)(h).

¹¹⁵ See: *ibid*, s 1(a) & (h) .

¹¹⁶ See: *ibid*, s 24 for the principles and lawful basis governing processing of Personal data.

¹¹⁷ See: *ibid*, ss 34–38.

¹¹⁸ See generally: *Ibid* part X and XI.

¹¹⁹ *Ibid*, s 43.

independent authority with significant power to issue binding regulations and guidance. It can determine how adequate foreign jurisdictions and transfer mechanisms are, conduct investigations, and impose administrative penalties.¹²⁰ The NDPC is also tasked with engaging in international and regional cooperation on data protection and cross-border transfers, making it the key authority for managing Nigeria's CBDF system.¹²¹ This institutional setup shows a preference for administrative discretion and proactive regulatory control instead of relying on automatic or market-driven data movement.

Nigeria's implementing tool, the subsidiary legislation made pursuant to the NDPA, further enhances this awareness of sovereignty. The General Application and Implementation Directive 2025 (GAID) clearly states that data protection is a required step for effective national and cross-border data flows. It highlights data sovereignty, national interests, and treaty obligations as critical factors in regulating data transfers.¹²² The GAID also explains the adequacy-based framework for cross-border transfers and subjects transfers from jurisdictions without adequacy recognition to closer scrutiny and consent-based safeguards.¹²³ These provisions emphasize the strategic importance of personal data in crucial economic and governance areas and highlight the NDPC's role in balancing openness with control.

From the perspective of AfCFTA alignment, Nigeria's legal and normative framework generally aligns with the Protocol and the Annex on Cross-Border Data Transfers, recognizing cross-border data flows as legitimate and necessary for digital trade. However, the NDPA and GAID place more emphasis on regulatory discretion, adequacy assessment, and maintaining sovereignty than on

¹²⁰ See: *ibid*, ss 4–7 which establishes the Nigerian Data Protection Commission.

¹²¹ See: *ibid*, s 5(j).

¹²² See: *General Application and Implementation Directive (GAID)*, 2025 art 3(1).

¹²³ See: *ibid* arts 45 & Sch 5.

automatic or unconditional data movement.¹²⁴ This foundational stance does not prevent alignment with AfCFTA CBDF obligations, but it makes such alignment dependent on the practical exercise and coordination of regulatory discretion. The extent to which this conditional openness supports or limits AfCFTA-level interoperability will be evaluated in further analyses.

4.2.2 Substantive Regulatory Scope

The regulatory framework for Nigeria's cross-border data flow (CBDF) is shaped primarily by the transfer rules in the Nigeria Data Protection Act 2023 (NDPA) and its General Application and Implementation Directive 2025 (GAID). Both instruments also interact with other sector-specific regulations. This setup allows the NDPA to establish the baseline legality of cross-border transfers, while various sectoral regulations in sectors such as finance, telecommunications, and health shape the operational conditions under which data may be processed and transferred.¹²⁵

The NDPA uses a conditional model for allowing cross-border transfers of personal data. Section 41 establishes a general prohibition, rendering transfers lawful only where the conditions set out in the Act are satisfied.¹²⁶ This approach avoids both a blanket ban and a general data-localization requirement, while subjecting transfers to the safeguards contained in Part VIII.¹²⁷ According to section 42, transfers can take place if the receiving country or organization offers an adequate level of data protection as determined by the Nigeria Data Protection Commission (NDPC).¹²⁸ If adequacy is not established, section 43 allows transfers based on alternative safeguards. These

¹²⁴ Notably, the CBDF provision of the NDPA is drafted in negative, prohibition-first terms. By providing that a controller or processor “shall not” transfer personal data outside Nigeria unless specified conditions are met, the Act establishes a default ban with legality arising only by exception. This reflects a control-oriented regulatory design that prioritizes regulatory discretion and administrative oversight over automatic data mobility. See: *NDPA 2025*, *supra* note 112, s 41.

¹²⁵ For example, the CBN regulation on BVN operations requires that BVN data shall be store in Nigeria and shall not be routed across borders without the consent of the CBN. See: *Central Bank of Nigeria Regulatory Framework for Bank Verification Number (Operations) and watch-list for the Nigerian banking industry*, 2021 art 1.11(ii).

¹²⁶ *NDPA 2025*, *supra* note 112, s 41.

¹²⁷ See: *ibid* part VIII.

¹²⁸ See: *ibid*, s 42.

include binding contracts, approved codes of conduct, certification mechanisms, or explicit consent from data subjects, all under regulatory supervision of the NDPC.¹²⁹

The GAID puts these legal rules into practice by outlining how to assess adequacy and apply alternative safeguards. Article 45 and Schedule 5 introduce stricter accountability, documentation, and proportionality requirements for transfers to countries without adequate protections.¹³⁰

Together, the NDPA and GAID create a structured transfer framework that allows cross-border data flows while imposing regulatory safeguards. This matters for AfCFTA CBDF implementation because a conditional facilitation model aligns with the Protocol's emphasis on permitting cross-border transfers subject to legitimate public-interest safeguards, rather than relying on blanket prohibitions or localization mandates that would be difficult to reconcile with treaty-level trade commitments.

While neither the NDPA nor the GAID mandates data localization, their design creates indirect pressures for localization. The combined effects of adequacy assessments, approved safeguards, and stricter compliance requirements raise the costs associated with cross-border transfers, especially for sensitive data or high-risk activities. These pressures do not outright ban cross-border transfers but may encourage local data processing or storage if regulatory uncertainty or compliance challenges are perceived as significant.

Within this overarching framework, sector-specific regulations apply alongside the NDPA.¹³¹

While Section 3(2) of the NDPA removes certain processing activities from the Act's scope where justified by for national security, public order, or other public-interest considerations,¹³² the

¹²⁹ See: *ibid*, s 43.

¹³⁰ *GAID 2025*, *supra* note 121 art 45 & sch 5.

¹³¹ *NDPA 2025*, *supra* note 112, s 63. Priority only applies in cases of inconsistency which presupposes cocurrent applicability of other laws.

¹³² See: *ibid*, s 3(2).

continued application of sectoral data-governance rules reflects the preservation of sector regulators' independent statutory mandates and the NDPA's role as a baseline data-protection framework rather than an exclusive regulatory code.¹³³ As a result, sector regulators may impose additional operational requirements that condition how CBDF activities are carried out, provided such measures do not displace the NDPA's baseline transfer rules.¹³⁴

In the financial services sector, the Central Bank of Nigeria's regulations impose strict rules on data handling that interact with the NDPA transfer framework. The Regulatory Framework for Bank Verification Number (BVN) Operations puts stringent controls on biometric and identity-related financial data to reflect their sensitivity.¹³⁵ Although this framework does not specifically forbid cross-border transfers, it emphasizes centralized control and risk management, which tends to constrain offshore processing where regulatory oversight cannot be assured.¹³⁶ Similarly, the CBN's Guidelines on Point of Sale (POS) Card Acceptance Services impose data retention, security, and auditability obligations on payment processors.¹³⁷ Although these requirements do not mandate data localization, they condition cross-border processing on the ability of regulators to exercise effective oversight, thereby narrowing the range of practically viable transfer mechanisms under sections NDPA.

¹³³ *Central Bank of Nigeria (CBN) Act*, 2007, s 2(d), 33; *Nigerian Communications Act*, 2003, ss 4, 70, 146–147; *NDPA 2025*, *supra* note 112, ss 41–43; *GAID 2025*, *supra* note 121 art 3.

¹³⁴ *NDPA 2025*, *supra* note 112, s 63; *GAID 2025*, *supra* note 121 art 4.

¹³⁵ See generally: *CBN Revised Regulatory Framework for BVN*, *supra* note 124.

¹³⁶ See generally: *Ibid* art 1.11 and 1.12.

¹³⁷ Although the Central Bank of Nigeria Guidelines on Point of Sale (POS) Card Acceptance Services (2011) retain historical relevance, contemporary CBN regulation of POS operations is primarily expressed through subsequent payment-system reforms, including the Payment Terminal Service Aggregator (PTSA) regime and related CBN circulars. These instruments require payment service providers to route POS transactions through licensed aggregators and comply with enhanced reporting, monitoring, and supervisory obligations, which operationally reinforce data retention, security, and auditability requirements. See: *Central bank of Nigeria Circular to all Payment Service Providers (PSPs) on connectivity to Payment Terminal Service Aggregators*, PSM/DIR/CON/CWO/051/117 2024 at 1.

National security concerns also narrow the scope of CBDF through binding executive orders. The Designation and Protection of Critical National Information Infrastructure Order 2024 identify certain sectors as critical and imposes stricter security and control obligations over associated data.¹³⁸ When considered alongside the NDPA's exclusions for national security,¹³⁹ and the GAID's focus on public-interest factors,¹⁴⁰ the Order indirectly creates constraints on cross-border data handling involving designated infrastructure. These constraints do not outright ban cross-border transfers, but they significantly limit the transferability of affected data where offshore hosting could threaten security or national control.

In the telecommunications and digital infrastructure sector, regulations under the Nigerian Communications Act add further constraints on CBDF practices. Obligations related to network integrity, lawful access, and cooperation with national security bodies affect how cross-border data can be routed and processed.¹⁴¹ Although these rules do not replace the NDPA's framework, they require that cross-border data arrangements comply with domestic regulatory access and service continuity needs, which influences how transfer options are implemented.

Overall, these sector-specific regulations do not create separate CBDF frameworks and are not overridden by the NDPA or the GAID. Their legal impact comes from independent statutes or the NDPA's preservation of public-interest regulations under section 3, not from any delegation within the data protection rules. Nigeria's CBDF regime is thus best understood as a multi-layered model where cross-border data flows are legally allowed but shaped by regulatory safeguards and sector-specific conditions. This matters for AfCFTA CBDF implementation because a conditional

¹³⁸ These sectors include, Power and Energy, Water, Banking, finance and insurance, Health, education, public administration, etc. See: *Designation and Protection of Critical National Infrastructure Order*, 2024.

¹³⁹ See *NDPA 2025*, *supra* note 112, s 3(2)(a)–(b).

¹⁴⁰ *GAID 2025*, *supra* note 121 arts 2–3.

¹⁴¹ *Nigerian Communications Act*, *supra* note 132, ss 70, 104, 146–157; *Lawful Interception of Communications Regulations*, 2019, ss 3-4,8.

facilitation model aligns with the Protocol's emphasis on permitting cross-border transfers subject to legitimate public-interest safeguards, rather than relying on blanket prohibitions or localisation mandates that would be difficult to reconcile with treaty-level trade commitments.

4.2.3 Institutional and Enforcement Mechanisms

The system governing cross-border data flows (CBDF) in Nigeria features a centralized data protection authority that functions within a multi-regulator landscape. The NDPA establishes the Nigeria Data Protection Commission NDPC as the main body responsible for overseeing personal data protection and cross-border transfers.¹⁴² However, the actual enforcement of CBDF rules relies on cooperation with sector-specific regulators, whose mandates overlap with data governance. This arrangement is key to evaluating Nigeria's alignment with the AfCFTA CBDF framework, which prioritizes regulatory cooperation, interoperability, and effective enforcement instead of strict harmonization.

The NDPC, created under Part II of the NDPA, serves as an independent supervisory authority with wide-ranging regulatory, investigative, and enforcement powers.¹⁴³ The Commission can issue binding regulations and guidance, conduct investigations, enforce sanctions, and assess the adequacy of foreign jurisdictions or transfer methods for cross-border data transfers.¹⁴⁴ These powers make the NDPC the main authority in Nigeria's CBDF system, responsible for translating legal protections into practical transfer conditions.

Beyond its domestic supervisory role, the NDPC is also tasked with international and regional collaboration on data protection issues. Section 5(j) of the NDPA allows the Commission to work with foreign data protection authorities and international organizations, especially regarding cross-

¹⁴² *NDPA 2025*, *supra* note 112, ss 4–5.

¹⁴³ *Ibid* part II.

¹⁴⁴ See *ibid*, ss 5–7, 42–43; *GAID 2025*, *supra* note 121 arts 45 & Sch. 5.

border data transfers and enforcement.¹⁴⁵ This role aligns with the AfCFTA Digital Trade Protocol and the Annex on Cross-Border Data Transfers, which highlight the importance of regulatory cooperation and mutual support in facilitating cross-border data flows while protecting public policy interests. However, the effectiveness of this role hinges on the NDPC's capacity, resources, and actual collaboration with other regulators.

Implementing CBDF obligations is made more difficult by the existence of independent sectoral regulators with their own mandates. In the financial services area, the Central Bank of Nigeria (CBN) oversees banks, payment service providers, and financial infrastructure, including essential data systems for regulation and consumer protection.¹⁴⁶ Similarly, the Nigerian Communications Commission (NCC) manages network operators and service providers in telecommunications and digital infrastructure, addressing issues like lawful access, network integrity, and security.¹⁴⁷ These regulators do not derive their authority from the NDPA, nor are they under the NDPC's authority.

Consequently, Nigeria's CBDF governance relies on coordination rather than hierarchy. Sectoral regulators continue to create and enforce rules that impact data management and system design within their areas, while the NDPC maintains authority over personal data protection and cross-border transfer safeguards. The NDPA and the GAID do not set a formal hierarchy or conflict-resolution process for the NDPC and sector-specific regulators, which leaves inter-regulatory coordination in CBDF issues to informal arrangements instead of binding legal frameworks. The NDPA does not mandate a coordination forum or a clearance mechanism for CBDF decisions, nor does it grant the NDPC priority over other statutory regulators.

¹⁴⁵ See *NDPA 2025*, *supra* note 112, s 5(j).

¹⁴⁶ *CBN Act 2007*, *supra* note 132, s 2(d), 33.

¹⁴⁷ See: *Nigerian Communications Act*, *supra* note 132, ss 4, 70, 146–147;

This division of authority affects how CBDF is implemented. When sectoral regulators impose requirements related to supervisory access, security, or control of infrastructure, data controllers may encounter conflicting compliance demands when organizing cross-border transfers. The lack of formal coordination mechanisms raises the risk of inconsistent regulatory signals, especially in sensitive sectors where CBDF decisions involve both data protection and specific supervisory matters. In such cases, the NDPC's adequacy assessments or approval of transfer safeguards may be limited by parallel sector requirements that complicate offshore processing.

From an AfCFTA alignment viewpoint, Nigeria's institutional setup shows both advantages and challenges. The presence of a centralized data protection authority with clear CBDF and international cooperation roles aligns well with the AfCFTA's focus on regulatory coordination and interoperability. However, the absence of formal mechanisms for inter-regulator coordination and shared decision-making diminishes the predictability and transparency of CBDF implementation. While AfCFTA obligations do not require member states to abolish sectoral regulation, they do imply a certain level of institutional coherence to prevent regulatory fragmentation from hindering cross-border data movement.

Thus, Nigeria's institutional structure and implementation strategies indicate that its CBDF alignment under the AfCFTA is influenced less by the range of domestic legal rules than by the ability of regulatory bodies to work together, communicate, and cooperate across sectors. Whether Nigeria's CBDF framework can achieve AfCFTA-level interoperability will largely depend on the improvement of inter-agency coordination methods and the effective execution of the NDPC's cooperation role, rather than simply expanding its statutory powers.

4.2.4 Rights and Digital Safeguards

Rights and digital safeguards are a key part of Nigeria's cross-border data flow (CBDF) system. They protect individual interests and serve as conditions for lawful data transfers. The Nigeria Data Protection Act 2023 (NDPA) views rights protection as an important aspect of data governance. It directly influences the legality and design of cross-border transfers. At the same time, the rights framework adds layers of discretion, complexity in enforcement, and uneven regulation. This can affect how predictable and compatible CBDF is under the AfCFTA framework.

Nigeria's rights-based framework acknowledges enforceable data subject rights for all personal data processing, including cross-border transfers. The NDPA guarantees rights such as access,¹⁴⁸ correction,¹⁴⁹ deletion,¹⁵⁰ limiting processing,¹⁵¹ data portability,¹⁵² and objection,¹⁵³ with specific limitations. These rights apply to personal data processed within Nigeria and data transferred abroad.¹⁵⁴ This means Nigerian data protection standards extend to other countries through conditions placed on data controllers. While this broad reach boosts individual protection, it also raises compliance demands for organizations handling cross-border transfers with Nigerian data subjects.

The NDPA's architecture on transfers strengthens the global application of these rights. Sections 42 and 43 require that cross-border transfers must provide an adequate level of protection or similar safeguards.¹⁵⁵ This inherently includes the protection of data subject rights in the receiving

¹⁴⁸ NDPA 2025, *supra* note 112, s 34(a) & (b).

¹⁴⁹ *Ibid*, s 34(c).

¹⁵⁰ *Ibid*, s 34(d).

¹⁵¹ *Ibid*, s 35.

¹⁵² *Ibid*, s 38.

¹⁵³ *Ibid* at 36.

¹⁵⁴ See *ibid*, s 2.

¹⁵⁵ *Ibid*, ss 42 & 43.

country. The General Application and Implementation Directive 2025 (GAID) supports this requirement by connecting assessments of adequacy and alternative safeguards to issues of enforceability, accountability, and access to legal remedies.¹⁵⁶ In this way, rights protection is a prerequisite for CBDF and not just a remedy after a transfer. However, the real enforcement of these rights after data is sent abroad relies heavily on cooperation with foreign regulators.

Consent has a limited and carefully controlled role in Nigeria's CBDF rights framework. While consent is seen as a legal basis for processing and, in specific situations, a means for transferring data, the NDPA and the GAID do not treat consent as absolute or as a replacement for structural safeguards.¹⁵⁷ The GAID limits the use of consent for cross-border transfers, especially in cases of power imbalances or higher risks. It requires consent to be informed, specific, and revocable. This approach aligns with the AfCFTA's focus on protecting privacy. However, it creates operational uncertainty for cross-border transfers, especially when consent is withdrawn after data has been shared or when assessing consent's validity across jurisdictions with different laws.

Nigeria's rights framework provides extra protection for sensitive personal data, such as health, biometric.¹⁵⁸ The NDPA requires stricter conditions and stronger security for handling this data. In the context of CBDF, these additional protections lead to increased scrutiny of transfer methods and a greater need for safeguards approved by regulators, especially when sensitive data goes to places without matching protections. Although these safeguards do not formally ban cross-border transfers, they create higher compliance demands for certain data types and may limit feasible transfer options.

¹⁵⁶ *GAID 2025*, *supra* note 121 arts 45 & Sch 5.

¹⁵⁷ See *NDPA 2025*, *supra* note 112, s 43(1)(a).

¹⁵⁸ *Ibid*, ss 30; 65.

Enforcement and remedies are crucial yet vulnerable elements of Nigeria's rights-focused CBDF safeguards. The NDPA gives the Nigeria Data Protection Commission (NDPC) the authority to investigate violations, impose fines, and demand corrective actions, while allowing data subjects to seek legal remedies.¹⁵⁹ These enforcement tools also apply to cross-border transfers affecting the rights of Nigerian data subjects. However, their success in international situations relies largely on cooperation with foreign regulators and the enforcement of decisions beyond Nigeria's borders. Without established cross-border enforcement practices or binding mutual assistance agreements, rights protection in CBDF contexts may be more effective on paper than in reality.

From an AfCFTA alignment standpoint, Nigeria's rights and digital safeguards framework generally fits with the Protocol's recognition of privacy and data protection as valid public policy goals that can shape CBDF obligations. The NDPA does not view rights protection as a strict barrier to data flow but as a series of conditions meant to encourage trust, accountability, and fairness in cross-border processing. Nevertheless, the extensive list of rights, the role of regulators in guarding against transfers, and the extra protection for sensitive data add layers of discretion and complexity, which can lower predictability for cross-border actors and complicate interoperability among State Parties with less rigorous rights standards.

Therefore, Nigeria's rights-based safeguards act as a conditional support system for CBDF rather than an outright facilitator of data movement. While they encourage data flows that comply with AfCFTA by embedding trust and accountability in transfer methods, they also reveal structural tensions between rights protection, regulatory discretion, and trade facilitation in a legally fragmented environment across the continent. These tensions highlight the limitations of rights-based safeguards as a sole solution for CBDF interoperability and emphasize the need for

¹⁵⁹ *Ibid*, s 6(f-g).

institutional coordination and cooperative measures, which will be explored further in the alignment assessment and subsequent chapters.

4.2.5 Socio-Economic and Technical Context

The socio-economic and technical context in which Nigeria’s cross-border data flow (CBDF) framework operates affects CBDF operability primarily through the way domestic legal design allocates compliance responsibilities and structures regulatory decision-making. Nigeria’s CBDF framework operates within a legal design that relies on coordination across multiple regulators rather than hierarchical control. While the NDPA and its implementing instruments establish a formal basis for cross-border transfers, they do not centralize CBDF governance exclusively within the NDPC.¹⁶⁰ Instead, the framework assumes concurrent regulatory authority, with sectoral regulators retaining mandates that intersect with data governance.¹⁶¹

This design allocates substantial compliance and assessment burdens to private actors. Data controllers and processors must satisfy NDPA transfer conditions while also navigating sector-specific regulatory requirements that affect how data may be processed or accessed across borders.¹⁶² Because these obligations are administered through multiple regulatory interfaces, CBDF operability depends less on the existence of lawful transfer mechanisms than on the ability of firms to reconcile overlapping and sometimes discretionary regulatory expectations.

The framework further relies on decentralised compliance assessment.¹⁶³ While adequacy determinations and transfer safeguards are anchored in the NDPA and its implementing

¹⁶⁰ *Ibid*, ss 41–43, 4(1).

¹⁶¹ See *ibid*, s 63; See also *GAID 2025, supra* note 121 arts 3, which provides for statutory remedy in respect of duple or multiple regulatory framework on data protection implying a recognition of multiple regulatory framework.

¹⁶² *NDPA 2025, supra* note 112, s 41(2)-(3) places responsibility on data controllers and processors to ensure and demonstrate lawful bases and safeguards for cross-border transfers.

¹⁶³ See *ibid*, s 41(2), which places the obligation to ensure lawful processing and the adoption of appropriate safeguards on data controllers and processors. In the context of cross-border data transfers, this framing allocates compliance assessment to the transferring entity at the point the transfer occurs, hence the description as “decentralised”.

instruments, their practical application occurs across multiple regulatory interfaces rather than through a single, uniform process. Although sectoral regulators may not adopt measures that directly contravene the NDPA, this principle functions primarily as a conflict-resolution mechanism and does not establish an operational hierarchy in favour of NDPC rules. Consequently, firms structuring cross-border data arrangements must account for overlapping regulatory requirements and manage coordination risks in practice.

From an AfCFTA alignment perspective, Nigeria's CBDF design remains formally compatible with the Digital Trade Protocol's approach to permitting cross-border transfers subject to legitimate public-interest safeguards.¹⁶⁴ However, reliance on regulatory layering, discretionary assessments, and decentralized coordination reduces predictability and complicates interoperability at the continental level.¹⁶⁵ While cross-border data flows are legally permitted in principle, the overall design places substantial coordination demands on private actors rather than resolving them through institutionalized mechanisms.

4.3.0 Kenya

Kenya provides a structured illustration of cross-border data flow governance within Africa through a consolidated statutory framework under the Kenya Data Protection Act 2019 (KDPA).¹⁶⁶ The Kenyan regime combines clearly articulated transfer conditions with a broader data protection architecture that recognizes consent as a lawful basis for processing, while assigning significant regulatory functions to the Office of the Data Protection Commissioner (ODPC).¹⁶⁷ Rather than

¹⁶⁴ See *AfCFTA Digital Trade Protocol*, *supra* note 13 art 20(1)-(2).

¹⁶⁵ *Annex on Cross-Border Data Transfers*, *supra* note 78 arts 16, 19 establishes non-restriction principle; transparency and interoperability objectives in CBDF governance.

¹⁶⁶ See *The Data Protection Act No. of 24 of 2019*, 2019 part VI, ss 48-50.

¹⁶⁷ See *ibid* at 48(1), 30(1)(a), 8(a), (c), (e).

relying on formal country-level adequacy determinations or a closed list of approved transfer instruments, the Act permits cross-border transfers where lawful processing grounds and appropriate safeguards are in place, with compliance assessed and enforced by an independent supervisory authority exercising delegated oversight and enforcement powers.¹⁶⁸

As East Africa's digital hub, Kenya plays a key role in cross-border digital services such as financial technology, telecommunications, cloud computing, e-commerce, and public services driven by data. This position has created ongoing demand for cross-border data movement while also raising concerns about privacy, sovereignty, and oversight. Kenya's domestic framework for cross-border data reflects these competing needs.¹⁶⁹ It aims to facilitate international data transfers while enforcing strong prior controls based on consent, legal conditions, and the discretion of supervisors.¹⁷⁰

Following the analytical framework earlier described, Kenya's domestic framework for cross-border data is analyzed in this section across five dimensions. First, it looks at the legal and normative bases of Kenya's data protection system. Second, it evaluates the regulatory scope for cross-border transfers, including legal conditions and consent rules. Third, it examines the institutional mechanisms and practical roles of the ODPC. Fourth, it assesses rights and digital protections as both enablers and limits on cross-border data flows. Finally, it situates Kenya's data regime within its regulatory and institutional design context by examining how the allocation of compliance burdens, the degree of regulatory layering, and reliance on decentralized compliance assessment mechanisms affect the operability of cross-border data governance under domestic law.

¹⁶⁸ See *ibid* at 48(1)(a)–(c), 5(1), 8(d), (f). Notably, under section 48, country-list adequacy mechanism is not provided.

¹⁶⁹ See *ibid*, ss 3 and 48.

¹⁷⁰ See *ibid*, ss 48–49.

This organized analysis lays the groundwork for a comparative overview in the following sections of this chapter, without making assumptions about whether Kenya meets agreements related to the AfCFTA. Kenya's domestic framework is assessed as a unique regulatory model in its own right, with design choices that have significant implications for interoperability across the continent and the integration of digital trade.

4.3.1 Legal-Normative Foundations

Kenya's legal framework for cross-border data flows (CBDF) is mainly set by the KDPA and the Data Protection (General) Regulation 2019.¹⁷¹ It establishes data protection as a legal right and regulates international transfer of personal data through stipulated legislative requirements.¹⁷² The Act applies to how data controllers and processors in Kenya handle personal data. It also covers data processing outside Kenya that relates to individuals located in Kenya irrespective of the processor's location.¹⁷³ This means it extends its legal reach into CBDF scenarios as designed by the law.

The KDPA asserts its authority by recognizing data protection as a legal right. It places obligations on data controllers and processors regardless of where the processing occurs.¹⁷⁴ Personal data is defined broadly, including any information about an identifiable person.¹⁷⁵ Processing encompasses various activities like collection, storage, use, disclosure, and transfer, including sending data outside Kenya.¹⁷⁶ As a result, cross-border data transfers are not treated as an exception, but as a regulated activity under the Act.

¹⁷¹ Notably, multiple subsidiary legislations have been made pursuant to the KDPA majority of which do not have any provisions on CBDF, other than the Data Protection (General) Regulations 2021. See *The Data Protection (General) Regulations, Legal Notice No. 263, 2021*.

¹⁷² See *Kenya Data Protection Act, supra* note 165 at 3, 48–49.

¹⁷³ *Ibid.*, s 4(b)(ii).

¹⁷⁴ *Ibid.*, s 4(b)(i).

¹⁷⁵ See *ibid.*, s 2.

¹⁷⁶ *Ibid.*

The KDPA lays out the rules for international data transfers directly in the legislation. Part VI specifies that personal data can only be transferred outside Kenya if the data controller or processor has provided adequate safeguards and met at least one of the legal conditions for transfer.¹⁷⁷ These conditions include the consent of the data subject, necessity for contractual or legal reasons, public interest needs, or other situations explicitly recognized by the Act.¹⁷⁸ This legal framing means that the legality of CBDF hinges on meeting defined legal standards rather than seeking regulatory permission. Consent plays a crucial role in Kenya's CBDF framework. The KDPA defines consent strictly as a clear and informed decision made by the data subject.¹⁷⁹ It limits when consent can be used as a valid legal basis. Plus, the Act elevates consent to a crucial safeguard in CBDF situations involving sensitive personal data.¹⁸⁰

The KDPA creates a system for protecting sensitive personal data differently from ordinary personal data, imposing stricter legal controls.¹⁸¹ Sensitive personal data includes, among other things, health information, biometric data, genetic data, and data about race, ethnicity, or religious beliefs.¹⁸² In CBDF situations, this distinction matters because it leads to stricter transfer requirements and emphasizes the importance of consent and safeguards for international data flows that involve such category of sensitive data.

The framework also outlines the role of the ODPC to monitor compliance, investigate issues, issue enforcement notices, and take corrective steps if the Act is violated.¹⁸³ Regarding CBDF, the Commissioner can suspend or block a data transfer outside Kenya if the legal conditions for

¹⁷⁷ *Ibid*, ss 48–49.

¹⁷⁸ See *ibid*, ss 48–49.

¹⁷⁹ *Ibid*, ss 2, 32.

¹⁸⁰ Section 49 clearly states that transfers of sensitive personal data outside Kenya must be accompanied by the data subject's consent, along with other legal safeguards. See *ibid*, s 49(1)(c).

¹⁸¹ *Ibid*, ss 44–47.

¹⁸² See *ibid* at 2.

¹⁸³ *Ibid*, ss 8–9.

transfer are not met or if the rights and freedoms of data subjects are at risk.¹⁸⁴ These powers support legal norms but do not change the legislative requirements for transfer legality.

The KDPA also grants the Cabinet Secretary the power to make subsidiary legislations for implementing its provisions.¹⁸⁵ However, this authority does not allow for changing the legal requirements for cross-border transfers, and any regulations created are meant to support legal norms, not to establish new rules for CBDF.¹⁸⁶

Consequently, and summarily, Kenya's legal foundations create a statute-first approach to CBDF. The conditions for international data transfers are embedded in its primary legislation, firmly anchored in a strict view of consent, and supported by a system for protecting sensitive data. Regulatory authority of the ODPC focuses on overseeing and enforcing these legal standards rather than granting case-by-case discretionary authorization for cross-border data transfers.¹⁸⁷ This legal arrangement emphasizes certainty and individual rights in managing CBDF, shaping how regulatory scope and institutional actions are explored in the following sections.

4.3.2 Substantive Regulatory Scope

By embedding the core transfer rules in primary legislation, the KDPA emphasizes that the legality of cross-border transfers depends primarily on compliance with statutory conditions.¹⁸⁸ Part VI of the KDPA governs the transfer of personal data outside Kenya. It permits such transfers only where the data controller or processor has implemented appropriate safeguards and satisfied at least one

¹⁸⁴ See *ibid*, s 49(3).

¹⁸⁵ The power to make subsidiary legislation is granted to Cabinet Secretary. See *ibid* at 71.

¹⁸⁶ See *ibid* at 71(3).

¹⁸⁷ The implication of section 49 is that cross-border data transfers are permitted without prior authorisation, while empowering the Commissioner to require a transferring person to demonstrate the existence of appropriate safeguards and, following investigation, to suspend or prevent further transfers. See *ibid*, s 49; Also, it should be noted that while this is true generally, there are a few narrow specific exceptions requiring prior approval, including for civil registration data. See *Data Protection (Civil Registration) Regulations, Legal Notice No 196 of 2020*, 2020, s 38.

¹⁸⁸ *Kenya Data Protection Act*, *supra* note 165 part VI.

of the statutory transfer conditions set out in the Act.¹⁸⁹ Section 49 identifies the principal legal gateways for cross-border transfers, including consent of the data subject, necessity for contractual performance or legal proceedings, public interest considerations, and other specified legal bases.¹⁹⁰

These gateways operate cumulatively with the safeguard requirement, producing a two-part legality test that combines substantive justification with protective measures.¹⁹¹

Consent plays an important role within this framework. The KDPA defines consent narrowly as a clear, voluntary, specific, and informed expression of the data subject's wishes,¹⁹² a definition that applies to all processing activities, including cross-border transfers. In the context of sensitive personal data, the Act further tightens the substantive conditions for transfer by requiring the data subject's consent in addition to the satisfaction of other statutory safeguards.¹⁹³ Sensitive personal data is defined broadly to include, among other categories, health, biometric, and genetic data, as well as data revealing race, ethnicity, or religious beliefs,¹⁹⁴ thereby narrowing the range of permissible transfer gateways for such data.¹⁹⁵

Alongside these legal gateways, the KDPA requires that appropriate safeguards be in place for cross-border transfers.¹⁹⁶ While the Act does not exhaustively define the content of such safeguards, it contemplates the use of contractual, organizational, and other protective measures to ensure a level of protection consistent with domestic standards.¹⁹⁷

Section 49(3) reinforces these substantive conditions by permitting restrictions on cross-border transfers where the statutory requirements for legality are not met or where the transfer poses a

¹⁸⁹ *Ibid*, ss 48–49.

¹⁹⁰ See *ibid*, s 49(1).

¹⁹¹ *Ibid*, s 49(2).

¹⁹² *Ibid*, s 2.

¹⁹³ *Ibid*, s 49(1)(c).

¹⁹⁴ See *ibid*, s 2.

¹⁹⁵ See *ibid* at 46.

¹⁹⁶ See *ibid*, s 48.

¹⁹⁷ See *ibid*, s 48(1)-(2) read together with s 41.

risk to the rights and freedoms of data subjects.¹⁹⁸ The Data Protection (General) Regulations 2021 further operationalises these substantive rules by clarifying compliance obligations, registration requirements, and procedural safeguards, without altering the underlying legal gateways or replacing the conditions set out in the Act.¹⁹⁹

While the KDPA constitutes the primary legal framework for cross-border data transfers, additional substantive constraints apply to some class of data set. In particular, the Data Protection (Civil Registration) Regulations 2020 impose a prior approval requirement for the transfer of civil registration data outside Kenya.²⁰⁰

Overall, Kenya's CBDF framework establishes a controlled yet predictable system of cross-border transfers grounded in statutory gateways, strict consent requirements for sensitive data, and limited sector-specific constraints. By anchoring transfer legality in primary legislation while allowing narrowly tailored exceptions for high-risk data categories, the framework maintains substantive legal clarity without eliminating regulatory discretion. The implications of this layered substantive design for institutional coordination and enforcement are examined separately in the following section.

4.3.3 Institutional and Enforcement Mechanisms

Kenya's framework for implementing cross-border data flow (CBDF) obligations centers on a main supervisory authority. This authority operates independently and works within a coordinated legal structure. The Kenya Data Protection Act 2019 (KDPA) establishes the Office of the Data Protection Commissioner (ODPC) as the key institution responsible for managing data protection obligations, including those related to international data transfers.²⁰¹

¹⁹⁸ See *ibid*, s 49(3).

¹⁹⁹ *Kenya Data Protection (General) regulation*, *supra* note 170 part VII.

²⁰⁰ *Kenya Data Protection (Civil Registration) Regulations 2020*, *supra* note 186, s 38.

²⁰¹ See *Kenya Data Protection Act*, *supra* note 165, s 5.

The KDPA designates the ODPC as a body corporate.²⁰² In performing its duties, the Commissioner must act independently, guided only by the Constitution and the law²⁰³. The Commissioner's statutory duties include enforcing the Act, monitoring compliance among data controllers and processors, investigating and inspecting, issuing directions, and promoting best practices in data protection across the economy.²⁰⁴

A key aspect of Kenya's institutional design is that there is no general licensing or approval requirement for cross-border transfers under the KDPA, except for a few specific class of data.²⁰⁵ The legality of transfers is mainly based on adherence to the conditions outlined in Part VI of the Act, with institutional action occurring when those conditions are violated or poorly implemented.²⁰⁶ The Commissioner can take corrective measures through investigations and enforcement instead of requiring prior approvals for transfer legality.²⁰⁷

The KDPA also includes formal mechanisms for coordination between regulatory bodies. The Commissioner can collaborate with other organizations to effectively carry out the Act's functions, including working with national security agencies when necessary²⁰⁸ Additionally, the Act allows the delegation of specific duties to another regulator created by an Act of Parliament.²⁰⁹ This provision supports coordinated oversight in areas where data protection overlaps with specialized regulatory functions. Such a design helps reduce regulatory fragmentation by aligning CBDF supervision with sectoral expertise while maintaining the ODPC's overall supervisory role.

²⁰² *Ibid*, s 5(1).

²⁰³ *Ibid* at 8(3).

²⁰⁴ *Ibid*, ss 8–9.

²⁰⁵ See *Kenya Data Protection (Civil Registration) Regulations 2020*, *supra* note 186, s 38.

²⁰⁶ See *Kenya Data Protection Act*, *supra* note 165, ss 48–49.

²⁰⁷ See *ibid*, s 49.

²⁰⁸ See: *ibid*, s 8(2) & 9(2)).

²⁰⁹ *Ibid*, s 10.

Enforcement powers are the main way CBDF obligations are carried out in practice. The Commissioner has the authority to conduct investigations, summon individuals, request information, issue administrative orders, and impose penalties for violations of the Act.²¹⁰ In particular, regarding cross-border transfers, the Commissioner can suspend or stop the transfer of personal data outside Kenya if the conditions for transfer are not met or if the transfer could harm the rights and freedoms of data subjects.²¹¹ This authority for injunctions reinforces compliance with transfer conditions through post-incident control.

Institutional implementation is further bolstered by procedural safeguards and judicial review. The Commissioner's decisions, including those on enforcement and penalties, can be appealed to the High Court.²¹² This adds a rule-of-law framework to CBDF enforcement and limits regulatory discretion.

Overall, Kenya's institutional and implementation framework demonstrates a supervisory-enforcement model based on statutory authority, limited discretion, and coordination instead of a complete prior licensing system. The ODPC has significant powers, but these are defined by law. Compliance with CBDF is mainly enforced through investigations, corrective measures, and judicial reviews. This institutional setup ensures legal certainty by linking transfer legality to the law while also depending on effective coordination and enforcement ability. These factors directly impact rights protection and the functionality of cross-border data flows, which will be discussed in the next section.

²¹⁰ *Ibid* at 9, 62–63.

²¹¹ *Ibid*, s 49(3).

²¹² See *ibid*, s 64.

4.3.4 Rights and Digital Safeguards

Kenya's cross-border data flow (CBDF) regime includes rights protection and digital safeguards. The KDPA contains a clear list of data subject rights that apply whether personal data is processed in Kenya or transferred abroad.²¹³ This implies that rights protection in cross-border situations is a legal matter, not just a regulatory choice.

The KDPA grants data subjects important rights, such as the right to be informed about how their personal data is used,²¹⁴ the right to access their data,²¹⁵ the right to correct inaccuracies,²¹⁶ the right to delete their data,²¹⁷ and the right to object to processing under certain conditions.²¹⁸ These rights place corresponding responsibilities on data controllers and processors to ensure that cross-border processing does not reduce the protection for data subjects.²¹⁹ In CBDF situations, the right to be informed is especially important. It mandates that data subjects are informed about processing purposes, who receives their data, and whether their personal data might be sent outside Kenya.²²⁰ Consent serves as both a lawful basis for processing and transfer and as a protective measure for rights within Kenya's CBDF framework.²²¹ The KDPA defines consent strictly, requiring it to be clear, voluntary, specific, and informed.²²² If consent is used to justify an international transfer, these conditions limit how consent can be obtained and restrict the use of bundled or implied consent. Additionally, the Act allows data subjects to withdraw consent at any time, subject to contractual and legal limits.²²³ In CBDF cases, this right adds a level of uncertainty to cross-border

²¹³ *Ibid*, s 26.

²¹⁴ See *ibid*, s 26(a).

²¹⁵ *Ibid*, s 26(b).

²¹⁶ See *ibid*, s 26(d).

²¹⁷ *Ibid*, s 26(e).

²¹⁸ *Ibid*, s 26(c).

²¹⁹ *Ibid*, s 48.

²²⁰ See *ibid*, s 29.

²²¹ *Ibid*, s 30(1).

²²² *Ibid*, s 2.

²²³ *Ibid* at 32(2).

transfers, as withdrawing consent can affect the legality of processing that takes place outside Kenya.

The KDPA also strengthens rights protection in CBDF situations by enforcing stricter safeguards for sensitive personal data.²²⁴ Transferring such data internationally requires the data subject's consent in addition to meeting other legal safeguards.²²⁵ This approach reflects the idea that certain types of data deserve more protection when transferred across borders.

Digital safeguards under the KDPA are expressed through statutory obligations and supervisory enforcement. Data controllers and processors must implement appropriate technical and organizational measures to protect personal data from unauthorized access, loss, or misuse.²²⁶ These requirements apply to both domestic and cross-border processing and cover entities that send personal data outside Kenya. In CBDF scenarios, the need for appropriate safeguards is a continuous duty rather than a one-time compliance check. This reinforces the expectation that data protection standards remain high throughout the data lifecycle, even after transfer.

The Act also establishes mechanisms for accountability and enforcement that are vital for protecting rights in cross-border cases. Data subjects can file complaints with the Office of the Data Protection Commissioner if they believe their rights have been violated, including regarding international transfers of their personal data.²²⁷ The Commissioner can investigate complaints, issue enforcement and penalty notices, and impose administrative fines when violations occur.²²⁸ These remedies apply regardless of whether the processing occurred in Kenya or abroad, as long as it falls within the Act's territorial scope.

²²⁴ See *ibid* part V.

²²⁵ See *ibid*, s 49.

²²⁶ *Ibid*, s 41.

²²⁷ *Ibid*, s 56.

²²⁸ *Ibid*, ss 9, 62–63.

Judicial oversight further supports rights and safeguards in CBDF scenarios. Decisions made by the Commissioner, including those on enforcement and penalties, can be appealed to the High. This appeal process integrates data protection enforcement into the larger judicial system and adds another level of accountability where cross-border processing raises rights issues.

Overall, Kenya's framework for rights and digital safeguards offers strong legal protections in CBDF situations through enforceable data subject rights, strict consent rules, extra safeguards for sensitive data, and accessible remedies. While this structure enhances rights protection and legal accountability, it also introduces potential challenges for cross-border data flows, especially if consent is withdrawn or if it is difficult to maintain equivalent safeguards across different jurisdictions. The effectiveness of these safeguards in practice relies on institutional capacity and enforcement, as explored in the following socio-economic and technical analysis.

4.3.5 Socio-Economic and Technical Context

The operability of Kenya's cross-border data flow (CBDF) regime is shaped primarily by the structural features of its legal design rather than by empirical enforcement outcomes or levels of technical development. Under the Kenya Data Protection Act 2019 (KDPA), cross-border data governance is organised around statutory transfer gateways, safeguard requirements, and supervisory oversight, with primary responsibility for compliance resting on data controllers and processors.²²⁹ This design choice frames operability as a function of how legal obligations are allocated and coordinated within the regulatory architecture.

A central feature of the KDPA is the allocation of compliance and assessment burdens to regulated entities. Controllers and processors are required to determine, at the point of transfer, whether statutory conditions are satisfied and whether appropriate safeguards are in place.²³⁰ With the

²²⁹ *Ibid.*, ss 48, 49.

²³⁰ *Ibid.*, s 48(1).

exception of a few class of data such as civil registry data, the Act does not establish a single, centralized authorization process or requirement for cross-border transfers; instead, legality is assessed through decentralized compliance judgments subject to supervisory review.²³¹ This structure supports flexibility and scalability in CBDF governance but also places the operational burden of legal interpretation and risk management on regulated actors.

The degree of regulatory layering further shapes CBDF operability. While the KDPA embeds core transfer conditions in primary legislation, the general regulation adopted under the Act elaborate compliance obligations, registration requirements, and procedural safeguards.²³² In addition, dataset-specific approval requirements introduce targeted constraints within the general regime.²³³ These layers do not replace the statutory transfer gateways but increase the complexity of navigating CBDF obligations where general and specialized rules intersect.

The KDPA's reliance on decentralised compliance assessment mechanisms also affects operability.²³⁴ The open-textured requirement of "appropriate safeguards" allows for contextualised application across different transfer scenarios but leaves the adequacy of safeguards to be evaluated through supervisory oversight rather than predetermined standards.²³⁵ This design reduces rigidity but introduces legal uncertainty where regulatory guidance or sectoral clarification is limited, making operability contingent on how well decentralised assessments align with supervisory expectations.²³⁶

Taken together, these structural features indicate a CBDF regime that neither clearly enables nor categorically constrains operability. Kenya's legal design provides identifiable statutory gateways

²³¹ See *ibid*, s 49(1); See also *Kenya Data Protection (Civil Registration) Regulations 2020*, *supra* note 186, s 38.

²³² See *Kenya Data Protection Act*, *supra* note 165, s 71; See also *Kenya Data Protection (General) regulation*, *supra* note 170, ss 39–48.

²³³ *Kenya Data Protection (Civil Registration) Regulations 2020*, *supra* note 186, s 38.

²³⁴ *Kenya Data Protection Act*, *supra* note 165, s 48.

²³⁵ *Ibid*, s 49(1).

²³⁶ *Ibid*, s 8(c), 48–49, 71.

and avoids blanket prohibitions on cross-border transfers, while regulatory layering and decentralized assessment mechanisms introduce coordination and interpretation demands that may complicate implementation. Within the terms of Dimension 5, this places Kenya's CBDF framework in a position where operability is shaped by legal design trade-offs rather than by enforcement outcomes or infrastructural capacity.

4.4.0 South Africa

South Africa offers model based on a strong data protection law that was introduced earlier than in many other African countries. The Protection of Personal Information Act 2013 (POPIA) serves as the main legal framework for handling personal data and international transfers in South Africa.²³⁷ While key parts of POPIA took effect gradually, culminating in full enforcement from 2021, the Act represents a unified legal structure that integrates CBDF regulation into a wider set of data protection responsibilities and rights.

POPIA incorporates CBDF governance into South Africa's constitutional promise of privacy and self-determination regarding information. The rules around international data transfers under POPIA are shaped by the constitutional right to privacy. The Act enforces this right by requiring that cross-border data flows maintain a sufficient level of protection. Thus, South Africa does not see CBDF regulation as just a technical or trade issue; it views it as an extension of domestic privacy protections to international situations.

POPIA sets out specific requirements for cross-border transfers. These requirements depend on whether the recipient jurisdiction provides adequate protection, impose binding obligations on foreign recipients, or allow for alternatives like consent from data subjects or necessity-based

²³⁷ *Protection of Personal Information Act (POPIA) Act No 4 of 2013.*

reasons. These rules are found within the main legislation, not left to case-by-case regulatory approvals. This places CBDF governance securely within the legal framework. The Information Regulator is responsible for enforcing POPIA's obligations, including those related to cross-border information flows.

Institutionally, South Africa's CBDF system functions within a constitutional and administrative law context. This context shapes both regulatory authority and expectations for enforcement. POPIA creates the Information Regulator as an independent supervisory body with the power to investigate and correct issues. It also includes procedural safeguards and options for judicial review. Meanwhile, POPIA serves as the foundational legal framework for CBDF, with specific rules on confidentiality or data handling in different sectors working alongside it but not replacing its transfer requirements.

This section analyzes South Africa's domestic CBDF system using the same five-dimensional framework applied to Nigeria and Kenya. It will examine: (i) the legal-normative foundations of POPIA; (ii) the scope of regulations governing international data transfers and any localization-related constraints; (iii) institutional and implementation structures; (iv) rights and digital protections; and (v) the socio-economic and technical factors influencing CBDF in practice. This organized approach allows for a consistent evaluation of similarities and differences across these jurisdictions while taking into account South Africa's unique legal and institutional environment.

4.4.1 Legal-Normative Foundations

South Africa's legal framework for cross-border data flows (CBDF) is based on the Protection of Personal Information Act 2013 (POPIA). This law creates a rights-based system for handling personal information and governs international data transfers with clear statutory requirements. POPIA links CBDF governance to a broader promise of privacy protection. It enshrines the

constitutional right to privacy and extends that protection to transborder processing as a legal obligation instead of leaving it to regulatory discretion.

The authority of POPIA comes from its wide application and its inclusion of data protection principles, rights, and transfer conditions in one legislative document. The Act applies to the processing of personal information that a responsible party enters into a record, subject to specific jurisdictional and contextual limits.²³⁸ Personal information includes details about identifiable living individuals and identifiable legal entities, while “processing” refers to the collection, storage, sharing, and transmission of information, including across borders.²³⁹ Thus, cross-border data transfers are classified as a regulated form of processing within the Act, rather than as an exceptional activity needing ad hoc approvals.

POPIA places the legality of cross-border transfers squarely within the main law. Section 72 governs transborder information flows, stating that personal information may only be transferred outside South Africa if the recipient is bound by a law, corporate rules, or an agreement that offers a level of protection similar to that under POPIA.²⁴⁰ This requirement shows a preference for consistent data protection standards across borders rather than unrestricted data movement.

If it is not possible to establish an adequate level of protection, POPIA outlines specific alternative pathways for cross-border transfers.²⁴¹ These include situations where the data subject has consented to the transfer,²⁴² where the transfer is needed to fulfill a contract that involves the data subject,²⁴³ or where it is required for a contract that benefits the data subject.²⁴⁴ These pathways are legally defined and serve as conditions for transfer rather than optional permissions.

²³⁸ *Ibid*, s 3.

²³⁹ *Ibid*, s 1.

²⁴⁰ *Ibid*, s 72(a).

²⁴¹ See *ibid*, s 72(b)-(e).

²⁴² *Ibid* at 72(1)(b).

²⁴³ See *ibid* at 72(1)(d).

²⁴⁴ See *ibid* at 72(1)(e).

Generally, POPIA does not demand prior regulatory approval for cross-border transfers that follow section 72.²⁴⁵ However, POPIA includes specific prior-authorization rules for certain types of high-risk processing under other parts of the Act.²⁴⁶ While these may overlap with cross-border processing in some cases, they do not turn section 72 into a licensing-based CBDF system.

The legal framework is also influenced by POPIA's general conditions for lawful processing, which apply to all processing activities covered by the Act, including those with transborder transfers.²⁴⁷ These conditions include accountability,²⁴⁸ limits on processing,²⁴⁹ purpose specification,²⁵⁰ information quality,²⁵¹ security measures,²⁵² and participation by data subjects.²⁵³

In CBDF situations, these principles reinforce that responsible parties must ensure compliance with POPIA, even if personal information is handled by foreign entities. Specifically, the accountability principle places the main responsibility for compliance on the responsible party, including for cross-border processing.²⁵⁴

Institutionally, POPIA gives supervisory and enforcement powers to the Information Regulator, an independent body accountable to the National Assembly.²⁵⁵ The Regulator's role in CBDF governance is to oversee and correct rather than to determine the legality of transfers.²⁵⁶ The conditions for international data transfers are set by POPIA, with the Regulator responsible for monitoring compliance, investigating violations, and taking action when necessary.²⁵⁷

²⁴⁵ The legality of a transfer hinges on meeting the statutory conditions in that section, rather than receiving prior permission from the supervisory authority. See *ibid*, s 72.

²⁴⁶ See *ibid*, s 57.

²⁴⁷ See *ibid* chs 3, Part A.

²⁴⁸ See *ibid*, s 8.

²⁴⁹ See *ibid*, ss 9–12.

²⁵⁰ *Ibid*, ss 13–14.

²⁵¹ *Ibid*, s 16.

²⁵² See *ibid*, ss 19–22.

²⁵³ See *ibid*, ss 23–25.

²⁵⁴ *Ibid*, s 8.

²⁵⁵ See *ibid*, s 39.

²⁵⁶ *Ibid*, s 40.

²⁵⁷ *Ibid*, ss 72, 40.

Overall, South Africa's legal foundations create a CBDF system built on statutory protections, accountability, and a framework focused on adequate protection for transfers, embedded in primary legislation. By linking cross-border data flows to the need for adequate protection or specific legal pathways, POPIA emphasizes the continuity of rights protection across borders and reduces dependence on discretionary regulatory approvals. The effects of this framework on the scope and flexibility of international data transfers will be analyzed further in the examination of South Africa's regulatory approach.

4.4.2 Substantive Regulatory Scope

This section details the legal conditions under which personal information can be sent outside South Africa. The Act does not allow free data movement.²⁵⁸ Instead, it conditions these international transfers on compliance with legal safeguards that maintain protection for personal information once it leaves the country.²⁵⁹

Section 72(1)(a) sets the main transfer condition. It requires that the recipient of personal information in another country must be subject to laws, binding corporate rules, or agreements that offer an adequate level of protection for the information, similar to what POPIA provides.²⁶⁰ This requirement applies not only to the initial recipient but also covers further transfers. If information is protected by a binding agreement, that agreement must include safeguards for any additional transfers to third parties in other countries.²⁶¹ Thus, the adequacy requirement constrains both primary and onward cross-border data flows.

²⁵⁸ See generally *ibid*, s 72.

²⁵⁹ *Ibid* at 72(1)(a).

²⁶⁰ *Ibid*, s 72(1)(a).

²⁶¹ *Ibid* at 72(1)(a)(ii).

POPIA does not create a formal system for determining adequacy or provide jurisdiction-wide adequacy listings from the supervisory authority.²⁶² It is the responsibility of the party transferring the data to ensure an appropriate level of protection through relevant laws or binding agreements.²⁶³ In this way, POPIA integrates CBDF governance into its main legislation, relying on responsible private practices instead of prior regulatory approvals. When the adequate-protection requirement in section 72(1)(a) cannot be satisfied, POPIA offers specific alternative methods through which cross-border transfers can still occur.²⁶⁴ These pathways serve as legal conditions that validate international transfers without being mere exceptions granted by the supervisory authority.

Consent is acknowledged within South Africa's CBDF framework,²⁶⁵ but its role is limited. While consent can be a legal basis for cross-border transfers when adequate protection is lacking, it is only one of several channels. It does not replace POPIA's broader accountability and compliance requirements.²⁶⁶ POPIA mandates that consent be voluntary, clear, and informed.²⁶⁷

POPIA does not call for general data localization rules or broad prohibitions on international data transfers.²⁶⁸ Its approach towards CBDF is flexible but conditional, allowing cross-border data flows when legal safeguards are in place, rather than enforcing local storage or processing as a default.²⁶⁹ However, the need for adequacy requirements, onward-transfer protections, and accountability may influence localization in practice when equivalent protections cannot be easily

²⁶² Instead, compliance with the adequacy requirement is measured against the criteria in section 72. See *ibid*, s 72.

²⁶³ See *ibid*, ss 8, 19–22, 72(1).

²⁶⁴ See *ibid*, s 72(1)(b)–(e).

²⁶⁵ *Ibid*, s 72(1)(b).

²⁶⁶ *Ibid*, s 8.

²⁶⁷ See *ibid*, s 1.

²⁶⁸ See *ibid*, s 72.

²⁶⁹ *Ibid*, s 72(1).

secured across countries.²⁷⁰ These implications stem from compliance risks and safeguard limits rather than explicit localization requirements in the Act itself.

Overall, South Africa's CBDF framework establishes a conditional transfer system based on an adequate-protection requirement, specified legal pathways, and ongoing accountability obligations. This matters for AfCFTA CBDF implementation because adequacy-oriented transfer models prioritize legal certainty and rights protection, but may offer less flexibility than the AfCFTA framework, which is designed to accommodate a wider range of safeguard-based justifications rather than a single benchmark of equivalence. By embedding transfer legality within section 72 of POPIA and applying key processing principles to cross-border situations, the framework aims to maintain data protection continuity without enforcing blanket localization rules. The mechanisms for implementing and enforcing these rules are discussed in the following section.

4.4.3 Institutional and Implementation Mechanisms

South Africa's institutional framework for the implementation and enforcement of cross-border data flow (CBDF) obligations is centered on the Information Regulator with jurisdiction throughout the Republic and responsibility for monitoring and enforcing compliance with POPIA, including provisions governing transborder information flows.²⁷¹

POPIA expressly provides for the independence and accountability of the Information Regulator.²⁷² The Regulator is required to perform its functions without fear, favour, or prejudice, and is accountable to the National Assembly, to which it must submit reports on its activities and

²⁷⁰ See *ibid*, ss 8, 72(1).

²⁷¹ *Ibid*, ss 39–40, 72.

²⁷² *Ibid*, s 39(b).

performance.²⁷³ These institutional guarantees frame the Regulator’s authority over both domestic and cross-border personal data processing.²⁷⁴

The Act confers on the Information Regulator a structured mandate covering complaints handling, investigation, and enforcement.²⁷⁵ Any person may submit a complaint to the Regulator alleging an interference with the protection of personal information, including interference arising from unlawful international data transfers contrary to section 72.²⁷⁶ Upon receipt of a complaint, the Regulator may conduct a preliminary investigation, initiate a full investigation, or take other steps provided under the Act.²⁷⁷

Implementation of CBDF obligations under POPIA follows an ex-post enforcement model rather than a system of prior authorization. Section 72 does not require responsible parties to obtain advance approval from the Information Regulator before transferring personal information outside South Africa.²⁷⁸ Instead, responsible parties bear the obligation to ensure that the statutory transfer conditions in section 72 are satisfied, subject to subsequent supervisory scrutiny by the Regulator.²⁷⁹

Where an investigation reveals non-compliance with POPIA, including unlawful cross-border transfers, the Information Regulator is empowered to issue enforcement notices requiring a responsible party to take specified remedial action or to cease processing activities.²⁸⁰ Failure to comply with an enforcement notice constitutes an offence under the Act and may trigger further sanctions.²⁸¹

²⁷³ *Ibid*, s 39(c), 40(1)(b).

²⁷⁴ *Ibid*, s 40(1)(g).

²⁷⁵ *Ibid*, s 40.

²⁷⁶ See *ibid*, s 74(1).

²⁷⁷ See *ibid*, ss 76–80.

²⁷⁸ See *ibid*, s 72.

²⁷⁹ See *ibid* at 72(1).

²⁸⁰ *Ibid*, s 95(1), 95(2).

²⁸¹ *Ibid*, s 103(1).

Judicial oversight is expressly embedded within POPIA's implementation framework. A responsible party served with an enforcement notice may appeal against that notice to the courts in accordance with the procedures set out in the Act.²⁸² It also anticipates institutional interaction and coordination in the course of enforcement. Where a complaint relates to matters falling within the jurisdiction of another regulatory body, the Information Regulator may refer the complaint or relevant aspects of it to that body for appropriate action.²⁸³ This referral mechanism reflects a model of coordinated oversight rather than exclusive regulatory control, particularly where CBDF intersects with sector-specific regulatory regimes.

Taken together, POPIA establishes an institutional and implementation framework in which CBDF legality is determined by statutory conditions set out in section 72 and enforced through a combination of complaints handling, investigation, enforcement notices, administrative penalties, criminal offences, and judicial oversight. The Information Regulator's role is supervisory and corrective, not constitutive of transfer legality, with enforcement mechanisms designed to ensure compliance after the fact rather than through prior licensing, except in specific instances. The implications of this enforcement-centered institutional design for the protection of data subject rights in cross-border contexts are examined in the subsequent analysis of rights and digital safeguards.

4.4.4 Rights and Digital Safeguards

POPIA grants data subject rights and places obligations on responsible parties as part of its conditions for lawful processing and its specific rights provisions.²⁸⁴

²⁸² *Ibid.*, ss 97–98.

²⁸³ *Ibid.*, s 78.

²⁸⁴ See *ibid* at 5, 8–25, 69–71.

One important safeguard is the requirement to notify data subjects when collecting personal information. This includes disclosing the purpose of collection and the recipients or types of recipients of the information.²⁸⁵ The right of access allows a data subject to check if a responsible party holds their personal information and to request access to that information.²⁸⁶ POPIA also recognizes a right to request correction, destruction, or deletion of personal information that is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or unlawfully obtained.²⁸⁷

A data subject can object to the processing of their personal information on reasonable grounds related to their situation.²⁸⁸ They can also object to processing for direct marketing purposes as specified in the Act.²⁸⁹

POPIA reinforces safeguards for sensitive data by banning the processing of “special personal information” unless there is a legal authorization.²⁹⁰

Digital security safeguards require responsible parties to ensure the integrity and confidentiality of personal information. They must take appropriate and reasonable technical and organizational measures to prevent loss, damage, unauthorized destruction, and unlawful access or processing.²⁹¹

If there are reasonable grounds to believe that an unauthorized person has accessed or acquired personal information, the responsible party must notify the data subject and the Information Regulator as soon as possible, following POPIA’s conditions.²⁹²

²⁸⁵ *Ibid* at 18(1)(a)-(f).

²⁸⁶ *Ibid*, s 23.

²⁸⁷ See *ibid*, s 24.

²⁸⁸ *Ibid*, s 11(3).

²⁸⁹ See *ibid*, s 69(3).

²⁹⁰ See *ibid*, ss 26-33.

²⁹¹ See *ibid*, s 19.

²⁹² *Ibid*, s 22.

Finally, POPIA offers a civil remedy by allowing a data subject (or the Regulator at the data subject's request) to file a civil action for damages against a responsible party for breaches of POPIA. This applies whether or not there is intent or negligence, subject to specified defenses.²⁹³

These rights and safeguards apply to all processing by responsible parties and work alongside POPIA's conditions for transborder transfers. This means cross-border data flow arrangements must be set up so that POPIA-compliant rights and safeguards can be practically exercised.²⁹⁴

From an AfCFTA perspective, South Africa's strength lies in the clarity and enforceability of its transfer conditions, while its limitation lies in the relative rigidity of its equivalence logic, which may not fully reflect the Protocol's conditional and context-sensitive facilitation model.

4.4.5 Socio-economic and technical context

This section examines how the operability of cross-border data flow (CBDF) governance in South Africa is shaped by the structural features of the POPIA. The POPIA applies uniformly to all responsible parties and operators, including those engaged in cross-border processing, and allocates primary compliance responsibility to the entity transferring personal information, irrespective of sector, size, or processing model.²⁹⁵

A notable feature of POPIA's legal design is the allocation of compliance and assessment burdens to responsible parties. The Act requires each responsible party to ensure that statutory conditions for transborder transfers are satisfied and that appropriate safeguards are in place, even where processing is carried out by operators or recipients outside South Africa.²⁹⁶ This design embeds CBDF operability within a uniform accountability framework that does not differentiate obligations based on organizational capacity or technical sophistication.

²⁹³ See *ibid*, s 99(1)-(2).

²⁹⁴ See generally *ibid*, ss 8, 18, 19, 22–24, 72.

²⁹⁵ *Ibid* at 8, 19, 72.

²⁹⁶ *Ibid* at 8, 19–21, 72.

POPIA further shapes operability through its reliance on decentralized CBDF compliance assessment mechanisms.²⁹⁷ The Act does not prescribe specific technologies, data-localisation architectures, or transfer models for cross-border processing.²⁹⁸ Instead, it establishes outcome-oriented legal standards, such as the requirement for an adequate level of protection and appropriate technical and organisational measures, that must be assessed by responsible parties in light of the circumstances of each transfer.²⁹⁹

The absence of a formal adequacy-listing or jurisdiction-designation system reinforces this decentralized design.³⁰⁰ POPIA requires responsible parties to determine whether foreign legal systems, binding agreements, or corporate arrangements provide the level of protection required under section 72, including for onward transfers to third parties in other.³⁰¹ This places continuing assessment obligations on transferring entities as part of the statutory transfer framework.

While POPIA does not impose general data-localization requirements or prohibit cross-border transfers by default, its design conditions transfer legality on compliance with statutory safeguards and accountability obligations.³⁰² Oversight by the Information Regulator operates as a corrective mechanism within this structure, without displacing the decentralized assessment model or introducing a system of case-by-case transfer authorization.³⁰³

Finally, POPIA's civil-liability provisions form part of the legal design shaping CBDF operability by allocating compliance exposure to responsible parties through strict statutory liability for unlawful processing, including unlawful transborder transfers.³⁰⁴ Taken together, these features

²⁹⁷ See *ibid*, s 72.

²⁹⁸ See *ibid*, ss 19, 72(1)(a).

²⁹⁹ *Ibid*, ss 19, 72(1).

³⁰⁰ *Ibid*, s 72.

³⁰¹ *Ibid*, s 72(1)(a).

³⁰² *Ibid*, ss 8, 19, 72.

³⁰³ *Ibid*, ss 39, 40, 72.

³⁰⁴ See *ibid*, s 99.

reflect a CBDF framework that permits cross-border data flows under clearly defined statutory conditions, while structurally placing the operational and interpretive burden of compliance on regulated entities through a decentralized and layered legal architecture.

4.5.0 Comparative Synthesis of Alignment and Misalignment

This section combines the domestic analyses of Nigeria, Kenya, and South Africa to identify patterns of agreement and disagreement in national cross-border data flow (CBDF) systems. It does not repeat the specific findings found in sections 4.2 to 4.4. Instead, it brings together those findings using the five-dimensional analytical framework from Chapter 2. This framework helps explain how differences in legal structure, institutional setup, and application logic lead to different CBDF results in otherwise similar data protection systems.

The comparative analysis indicates that divergence among the three regimes arises less from incompatible legal objectives than from differences in regulatory technique, guidance density, and institutional capacity. These forms of divergence are AfCFTA-relevant because they affect how easily cross-border transfers can be operationalized, not whether they are formally permitted.

At the level of legal foundations, the three countries share a common approach by adopting comprehensive data protection laws as the main legal basis for managing cross-border data flows.³⁰⁵ However, the domestic analyses show that this apparent similarity hides deeper differences in legal focus and legislative methods. South Africa's system firmly bases CBDF legality in primary laws and emphasizes consistent protection across borders. Nigeria's approach mixes statutory rules with a strong reliance on delegated instruments and sector-specific regulations, which creates a layered and complex legal hierarchy. Kenya finds itself in between,

³⁰⁵ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* art 21 requires each state party to adopt or maintain a legal framework on data protection.

with CBDF legality based on laws but carried out through significant administrative guidance and regulatory details. The key point is that while there is legal alignment, the way legal certainty is created and maintained varies.³⁰⁶

Differences become clearer when looking at the rules governing cross-border transfers. South Africa organizes its CBDF system around an adequate protection rule, with clearly defined statutory conditions, including controls on onward transfers. These conditions set the legal framework for allowing data mobility but with restrictions. Kenya also permits cross-border transfers under certain legal conditions, but the local analysis shows a greater reliance on consent and supervisory interpretation, especially in complex or large-scale processing situations. Nigeria's CBDF landscape is influenced not just by general data protection laws but also by sector-specific regulations and public-interest categories that limit certain data types and processing activities. As a result, while all three countries allow transfers in theory, the combined effect of Nigeria's sector-specific laws and Kenya's operational challenges can restrict cross-border data movement more than in South Africa.

The ways the three systems implement these rules further set them apart. Each country has established a central data protection authority tasked with overseeing CBDF compliance.³⁰⁷ However, the analyses show that the environments in which these authorities work differ significantly. South Africa has a legal enforcement system that relies on statutes, where CBDF legality is determined by laws and enforced through complaints, investigations, penalties, and appeals. In Kenya, the data protection authority plays a larger role in enforcement through guidance and case-by-case supervision, affecting compliance behavior. Nigeria's implementation

³⁰⁶ Isaac Juma & Bukola Faturoti, "Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice" (2025) *International Review of Law, Computers & Technology* 1–26 at 6–9.

³⁰⁷ *AfCFTA Digital Trade Protocol*, *supra* note 1 art 21(6) stipulates that each part shall endeavor to establish national data protection authorities or other relevant body for personal data protection.

landscape is more complicated, involving the interaction among the data protection authority, sector regulators, and executive orders, which increases coordination challenges and varies interpretive clarity. The main point here is that institutional differences arise not from a lack of regulatory bodies but from how enforcement is designed and how different agencies interact.³⁰⁸

In terms of rights and digital protections, the three systems show a relatively strong baseline consistency. All three recognize essential rights for data subjects,³⁰⁹ impose security obligations,³¹⁰ require notification in case of breaches,³¹¹ and have mechanisms for complaints.³¹² Still, the analyses suggest that the robustness and effectiveness of these protections differ. South Africa combines a strong rights framework with strict remedial measures, creating powerful incentives for compliance in CBDF situations. Kenya's protections appear solid but rely more on administrative enforcement and managing consent. Nigeria offers extensive protections, but they work within a complex regulatory environment that can lead to inconsistent application, especially when sector-specific rules overlap with general data protection requirements. The central point is that even though rights seem aligned, this does not ensure similar cross-border enforceability, which can depend on institutional effectiveness and legal clarity.³¹³

The social, economic, and technical context also shows how similar legal obligations can lead to different outcomes. In all three countries, CBDF rules are uniformly applied by law without distinctions based on sector or company size. However, the context analyses reveal that the way compliance responsibility is assigned, the structure of accountability, and access to institutional

³⁰⁸ Juma & Faturoti, "Enforcing data privacy in Kenya and Nigeria", *supra* note 2 at 6–9.

³⁰⁹ *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 art 6.

³¹⁰ *Ibid* art 8; *AfCFTA Digital Trade Protocol*, *supra* note 1 art 25.

³¹¹ *Annex on Cross-Border Data Transfers*, *supra* note 5 art 10.

³¹² *AfCFTA Digital Trade Protocol*, *supra* note 1 art 21(5).

³¹³ See generally A B Makulilo, "Data Protection Regimes in Africa: too far from the European "adequacy" standard?" (2013) 3:1 *International Data Privacy Law* 42–50 at 44–48.

support impact how CBDF rules function in practice. South Africa’s decentralized adequacy assessment model and strict civil liability standards place ongoing compliance responsibilities on entities involved. Kenya's emphasis on consent and regulatory mediation interacts with its growing digital economy, leading to uncertainty and scalability issues. Nigeria’s developing enforcement capacity and layered sectoral regulations increase compliance complexity and transaction costs for cross-border activities. These contextual features do not indicate legal misalignment by themselves, but they significantly influence how easily the countries’ systems can align in practice. Together, the comparative analysis shows that the misalignment in African CBDF governance is not mainly due to direct legal incompatibility among national laws. Instead, it stems from differences in regulatory approaches, institutional frameworks, and implementation strategies that transform similar legal commitments into varied real-world applications. While there is alignment in legislative intent and fundamental data protection principles, this alignment weakens when considering transfer mechanisms, enforcement structures, and practical application.³¹⁴ This distinction is critical for AfCFTA implementation: doctrinal incompatibility would necessitate legal reform, whereas operational divergence can often be mitigated through interpretive alignment, administrative guidance, and regulatory cooperation. This pattern of partial agreement and structural divergence lays the groundwork for section 4.6, which turns these qualitative insights into a diagnostic alignment scorecard, and for Chapter 5, which looks at how the AfCFTA Digital Trade Protocol may address or manage these differences.

³¹⁴ See Alex B Makulilo, “Myth and reality of harmonisation of data privacy policies in Africa” (2015) 31:1 Computer Law & Security Review 78–89 at 82–85; See also Graham Greenleaf & Bertil Cottier, “International and regional commitments in African data privacy laws: A comparative analysis” (2022) 44 Computer Law & Security Review 105638 at 6–9.

4.6.0 AfCFTA CBDF Alignment Scorecard and Diagnostic Findings

This section combines the comparative analysis from sections 4.2 to 4.5 into a scorecard. The scorecard evaluates functional compatibility with the AfCFTA CBDF benchmark rather than formal legislative similarity. Scores reflect the extent to which domestic regimes are able to permit predictable, safeguard-based cross-border data transfers, taking into account both legal structure and institutional operability. The scorecard does not measure overall data protection quality or rights robustness as independent values. This framework translates qualitative findings into organized indicators of structural alignment and alignment risk across domestic CBDF systems. The diagnostic scores in this section come from the anchor-based coding method described in Chapter 2. The coding criteria, evidence mapping, and decision rules for each analytical dimension are detailed in Appendix A.

Table 4.1: AfCFTA CBDF Alignment Scorecard (Diagnostic)

Analytical Dimension	Nigeria	Kenya	South Africa
Legal–Normative Foundations	3	4	5
Substantive Regulatory Scope	2	3	4
Institutional & Implementation Mechanisms	2	3	4
Rights & Digital Safeguards	3	4	5
Socio-Economic & Technical Context	2	3	4

Scale: 1 = structurally misaligned · 2 = weak alignment · 3 = partial alignment · 4 = strong alignment · 5 = high structural alignment

Source: Author’s diagnostic assessment based on sections 4.2–4.5 and the anchor-scale methodology in section 2.7.

The scorecard shows how closely the structures align with the AfCFTA CBDF benchmark instead of measuring actual enforcement results. Scores rely on domestic legal frameworks, institutional setup, and operational factors discussed in Chapter 4. Dimension 5 serves as an indicator of structural conditioning, rather than a measure of socio-economic development or technical expertise. Its score indicates how well domestic legal design features allocate operability risk and shape the feasibility of implementing AfCFTA-style cross-border data flow commitments once, they are in place.

Looking at the legal and normative foundations, all three jurisdictions show moderate to strong alignment, indicating a shared approach to comprehensive data protection laws as the main method for CBDF governance. South Africa's score of 5 reflects that CBDF legality is embedded in primary laws and that its adequacy-focused framework is coherent. Kenya's score of 4 reflects a statute-first approach that clearly allows cross-border transfers but relies more on administrative interpretation and regulatory guidance for implementation. Nigeria's score of 3 reflects legislative convergence paired with weaker normative consolidation, as CBDF governance spans statutes, delegated instruments, and sector-specific rules. Therefore, the scoring captures variations in how legal certainty is established, rather than showing a lack of legal grounds for CBDF.

In terms of regulatory scope, differences are clearer. South Africa's score of 4 reflects its conditional permissiveness model, which aligns well with AfCFTA logic by allowing CBDF subject to ongoing protection and controlled transfers. Kenya's score of 3 indicates a permissive statutory framework, but its effectiveness is limited by reliance on consent durability and oversight, especially in complex or large data flows. Nigeria's score of 2 shows the cumulative impact of sector-specific localization requirements, approval processes, and public-interest

designations that significantly limit CBDF functionality beyond the AfCFTA benchmark. The scoring here reflects variations in actual transfer potential, not just formal legality.

The institutional and implementation mechanisms dimension receives the lowest overall alignment. South Africa's score of 4 reflects a legally anchored, enforcement-focused model that includes investigative, remedial, and judicial review mechanisms, providing predictable CBDF governance, even if it is not explicitly designed for continental regulatory cooperation. Kenya's score of 3 reflects a regulator-driven implementation environment that offers flexibility but is heavily reliant on administrative capacity and discretion. Nigeria's score of 2 reflects a fragmented institutional setup involving various sector regulators and executive tools, which raises coordination costs and reduces predictability for cross-border operations. The scorecard thus highlights that institutional design—not simply having a regulator—is the main source of misalignment.

In terms of rights and digital safeguards, alignment is relatively strong across all three jurisdictions. South Africa's score of 5 shows a comprehensive rights framework along with strong remedial measures and clear accountability in CBDF contexts. Kenya's score of 4 indicates solid statutory rights and safeguards whose effectiveness largely depends on administrative enforcement and consent management. Nigeria's score of 3 shows essential rights and safeguards that are complicated by sectoral layers and varying levels of enforcement maturity. The generally high scores in this area confirm that differences in rights are not the main hurdle to AfCFTA CBDF harmonization.

The socio-economic and technical context dimension is scored conservatively. These scores do not evaluate development levels, infrastructure quality, or enforcement effectiveness. Instead, they reflect alignment risk, i.e., the degree to which domestic legal design features allocate operability

risk and shape the feasibility of implementing AfCFTA-style CBDF commitments based on current legal frameworks. South Africa's score of 4 indicates a context where uniform accountability, decentralized adequacy assessment, and strict liability reinforce ongoing protection rigor. Kenya's score of 3 indicates moderate alignment influenced by governance design centered on consent, which increases operational uncertainty without outright restrictions. Nigeria's score of 2 shows higher alignment risk due to extensive sectoral layering, raising transaction costs and complicating cross-border compliance even when transfers are allowed by law. Scoring this dimension is crucial because it connects the legal analysis to operability without slipping into measuring performance.

Looking at the scorecard as a whole provides three key insights. First, alignment is strongest at the principle and rights level but weakest in implementation and transfer abilities, suggesting that AfCFTA CBDF coordination will face more challenges from institutional and regulatory design than from doctrinal conflicts. Second, sectoral fragmentation, particularly when it adds localization or approval requirements, appears to be the most significant cause of misalignment. Third, regulatory logic is important: statute-based, adequacy-focused regimes show greater structural compatibility with the AfCFTA benchmark than consent-focused or heavily layered regulatory models.

Overall, the scorecard indicates that AfCFTA CBDF harmonization cannot assume uniform domestic standards. While alignment exists, it is inconsistent and varies across dimensions. Thus, the scorecard serves as a bridge between the comparative analysis in Chapter 4 and the recommendations in Chapter 5, where the discussion explores how AfCFTA institutions can facilitate CBDF alignment through sequencing, regulatory cooperation, and implementation strategies that consider capacity.

4.7.0 Conclusion

This chapter looks at domestic cross-border data flow (CBDF) rules in Nigeria, Kenya, and South Africa. It uses a structured, five-dimensional framework, comparing these rules against the AfCFTA Digital Trade Protocol and its Annex on Cross-Border Data Transfers. The analysis moves beyond mere assumptions to highlight that regulatory fragmentation in African CBDF governance is a real issue, patterned, and specific to different dimensions. Fragmentation is not just a talking point in discussions about African digital trade; it is a clear structural aspect of the current domestic systems.

The main finding of the chapter is that misalignment in domestic CBDF does not mainly come from direct conflicts in legal doctrines or a lack of strong data protection laws. All three countries have general data protection frameworks that recognize the legitimacy of cross-border data transfers and incorporate CBDF governance into their national laws. The strongest alignment is in the legal and normative foundations, where common principles of data protection, accountability, and individual rights are widely accepted. These areas are the easiest to coordinate on a continental level.

However, the analysis shows that this alignment weakens when moving from legal structures to regulatory practices. The differences are most noticeable in the actual scope of CBDF regulations, institutional mechanisms, and the socio-economic and technical conditions that affect real-world operations. Various sector-specific rules, approval processes, localization effects, fragmented institutional roles, and enforcement challenges limit cross-border data movement in ways that headline laws do not fully capture. This leads to different effective CBDF environments across jurisdictions, even when formal legal frameworks seem similar.

The diagnostic scorecard developed in section 4.6 summarizes these findings by translating qualitative analysis into structured indicators of alignment and potential misalignment. The scorecard shows that misalignment is uneven rather than total; each jurisdiction has areas of agreement as well as significant differences. Importantly, it highlights that misalignment is not random; it closely relates to specific regulatory approaches and institutional structures. Models focused on adequacy and anchored in statutes tend to work better with the AfCFTA CBDF benchmark than those centered around consent or those that heavily layer regulations. This is especially true in cases where sectoral rules create multiple barriers to cross-border data processing.

A key takeaway from this chapter is that achieving CBDF harmonization under the AfCFTA requires more than just aligning legal doctrines. Because misalignment stems not only from legal text but also from how institutions are designed and how they implement regulations, efforts to put the AfCFTA CBDF framework into action must consider differences in enforcement structures, regulatory cooperation, and socio-technical capacity. While converging on rights is important, it is not enough to ensure that systems can work together without mechanisms to address sector-specific fragmentation and support coordinated implementation.

This conclusion sets the stage for the rest of the thesis. Chapter 4 shows that domestic CBDF regimes in Africa are neither completely incompatible nor easily harmonized by applying uniform legal approaches. Instead, they exist within a spectrum of partial alignment shaped by unique regulatory logics and operational limits. These findings clarify that any effective strategy for implementing the AfCFTA CBDF must be tailored, and sensitive to institutional contexts, rather than one-size-fits-all.

Chapter 5 builds on this analysis. It shifts the focus from comparing systems to implementing solutions, looking at how AfCFTA institutions and tools might address the specific sources of misalignment identified in this chapter. By grounding its recommendations in a thorough comparative analysis, the thesis positions Chapter 5 as a targeted response to established challenges in achieving continental CBDF integration.

Chapter 5: Towards Operationalizing the AfCFTA CBDF Regime

5.1.0 Introduction

The earlier chapters of this thesis present two main findings. First, the AfCFTA Digital Trade Protocol and its annex on Cross-Border Data Transfers create a legal framework for the continent that allows cross-border data flows (CBDF) as a generally accepted aspect of digital trade. This is subject to clearly defined public policy safeguards, including protections for personal data, national security, and regulatory independence.

Second, the comparison of Nigeria, Kenya, and South Africa shows that domestic CBDF systems differ significantly in their legal forms, institutional structures, and implementation methods. This results in uneven adherence to AfCFTA CBDF standards.

However, the findings in Chapter 4 reveal that this variation doesn't simply divide into compliance and non-compliance. The AfCFTA CBDF framework does not enforce strict, automatic transfer rules or require uniform domestic laws. It instead uses principles-based obligations, regulatory cooperation, and adaptable implementation methods. Therefore, divergence may indicate different regulatory approaches, institutional development, or levels of governance, rather than a failure to meet AfCFTA commitments.

The differences noticed across the case studies create practical challenges, not just theoretical ones. Much of the variation discussed in Chapter 4 stems from how CBDF rules are applied and organized within domestic legal systems that have different institutional capabilities and regulatory approaches. These differences affect the conditions for cross-border data transfers without undermining the general permissive nature of the AfCFTA framework.

This chapter directly tackles that challenge. Its aim is not to revisit the specific AfCFTA CBDF obligations or to reiterate domestic differences already explored in detail. Instead, it looks at how

AfCFTA CBDF rules can be made legally and institutionally functional across diverse national systems while maintaining both the integrity of continental trade commitments and the regulatory independence acknowledged in the Protocol. This shifts the focus from assessment to finding legal solutions.

A key point of this chapter is that the AfCFTA CBDF regime is not designed as a traditional harmonization tool.³¹⁵ Neither the Digital Trade Protocol nor the CBDF Annex requires uniform domestic data protection laws, mandates a single transfer process, or sets up a supranational enforcement authority over national regulators.³¹⁶ Instead, the AfCFTA framework highlights shared principles, interoperability, regulatory cooperation, and technical assistance, while acknowledging differences in development levels and institutional capabilities among State Parties.³¹⁷ This approach reflects the legal and political realities of integrating at the continental level in an area that connects with constitutional rights, public administration, and changing technological landscapes.³¹⁸

With this context in mind, this chapter uses the concept of operational alignment to evaluate AfCFTA CBDF implementation. Operational alignment means that domestic legal systems can effectively realize AfCFTA CBDF commitments, particularly regarding the allowance of cross-border data transfers and the continuity of safeguards, without needing to have identical legal rules or enforcement methods. This concept is not an official term but an understanding derived from

³¹⁵ As Burri and Kugler explains, modern digital trade agreements often pursue coordination rather than harmonisation, preserving domestic regulatory autonomy. See generally Mira Burri & Kholofelo Kugler, “Regulatory autonomy in digital trade agreements” (2024) 27:3 *Journal of International Economic Law* 397–423 at 399–402.

³¹⁶ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* arts 20–24; *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 arts 15–21.

³¹⁷ See generally African Union, *Guidelines for Integrating Data Provisions in Protocols on Digital Trade* (2023), online: <https://au.int/sites/default/files/documents/44807-doc-Guidelines-Integrating-Data-Digital-Trade-ENG-V3_161.pdf> at 25–30.

³¹⁸ See Alex B Makulilo, “Myth and reality of harmonisation of data privacy policies in Africa” (2015) 31:1 *Computer Law & Security Review* 78–89 at 84–86.

the structure of AfCFTA CBDF obligations that prioritize functionality, cooperation, and legal effectiveness over strict uniformity.³¹⁹

Operational alignment also recognizes that AfCFTA CBDF obligations focus more on cooperative and administrative implementation rather than hostile dispute resolution.³²⁰ Although the AfCFTA allows for dispute resolution, CBDF governance under the Digital Trade Protocol is primarily designed to develop through regulatory dialogue, capacity building, and gradual progression, especially in this early phase of implementation.³²¹ This institutional framework influences both the speed and form of alignment that can realistically be achieved.

The analysis unfolds in five steps. Section 5.2 identifies the root causes of CBDF misalignment within the AfCFTA legal system, separating systemic features from country-specific quirks. Section 5.3 redefines fragmentation by distinguishing between true doctrinal incompatibility and variations based on capacity and implementation, building on the diagnostic logic introduced in Chapter 4, and applied through the scoring methodology in Appendix A.

Section 5.4 explores the national and continental legal routes that can facilitate alignment without compromising regulatory autonomy. Section 5.5 examines how sequencing and timing influence AfCFTA CBDF implementation, suggesting that temporal differentiation is a key aspect of the Protocol's design. Finally, Section 5.6 considers what this model of operational alignment means for continental digital trade integration.

By emphasizing legal functionality over formal uniformity, this chapter argues that AfCFTA CBDF governance can operate effectively, even amid diverse domestic regulations. In this way,

³¹⁹ *AfCFTA Digital Trade Protocol*, *supra* note 2 arts 20–24; *Annex on Cross-Border Data Transfers*, *supra* note 2 arts 15–21.

³²⁰ *Agreement Establishing the African Continental Free Trade Area*, 2018 art 27; *AfCFTA Digital Trade Protocol*, *supra* note 2 arts 42–43.

³²¹ *Annex on Cross-Border Data Transfers*, *supra* note 2 art 21; African Union, *supra* note 3 at 40–41.

managed divergence is viewed as a strength of the AfCFTA CBDF regime, reflecting its integration strategy rather than a drawback.

5.2.0 Structural Sources of CBDF Alignment

The misalignment discussed in Chapter 4 does not happen randomly and cannot be blamed only on differing national policy choices.³²² Instead, it arises from structural features present in the relationship between the AfCFTA CBDF framework and local data governance systems.³²³ These features influence how continental CBDF commitments are turned into national laws and administrative practices.³²⁴ They also help explain why alignment outcomes differ, even when countries accept similar regulatory goals. As shown in the patterns observed in Chapter 4, misalignment is better understood as a result of structural interaction, not just isolated regulatory differences.

5.2.1 Normative Layering and Legal Pluralism

The misalignment discussed in Chapter 4 does not happen randomly and cannot be blamed only on differing national policy choices.³²⁵ Instead, it arises from structural features present in the relationship between the AfCFTA CBDF framework and local data governance systems.³²⁶ These features influence how continental CBDF commitments are turned into national laws and

³²² See generally Mira Burri, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation” (2017) 51 UC Davis Law Review 65–133 at 99–101.

³²³ See generally Franziska Sucker & Alexander Beyleveld, “African rules on cross-border data flows: The significance of regulatory convergence and the AfCFTA Digital Trade Protocol’s potential contribution” (28 February 2024) Rochester, NY, online: <<https://papers.ssrn.com/abstract=4741632>> at 9–13.

³²⁴ See *Agreement Establishing the African Continental Free Trade Area*, 2018 art 9.

³²⁵ See generally Mira Burri, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation” (2017) 51 UC Davis Law Review 65–133 at 99–101.

³²⁶ See generally Franziska Sucker & Alexander Beyleveld, “African rules on cross-border data flows: The significance of regulatory convergence and the AfCFTA Digital Trade Protocol’s potential contribution” (28 February 2024) Rochester, NY, online: <<https://papers.ssrn.com/abstract=4741632>> at 9–13.

administrative practices.³²⁷ They also help explain why alignment outcomes differ, even when countries accept similar regulatory goals. As shown in the patterns observed in Chapter 4, misalignment is better understood as a result of structural interaction, not just isolated regulatory differences.

5.2.2 Delegated Governance Density and Regulatory Technique

Another structural cause of misalignment relates to differences in regulatory methods, particularly the degree to which CBDF governance is carried out through delegated or administrative tools instead of primary legislation. Domestic systems vary widely in how they distribute regulatory details, discretion, and operational guidance among statutes, regulations, and administrative directives.³²⁸

The AfCFTA CBDF framework allows for this diversity. Neither the Protocol nor the CBDF Annex prioritizes statutory implementation over administrative or delegated forms of compliance.³²⁹ However, systems with dense layers of delegated governance often introduce greater discretion, variability, and interpretive flexibility into CBDF administration. As noted in the diagnostics of Chapter 4, these characteristics can lead to operational misalignment without indicating a doctrinal difference from AfCFTA CBDF commitments.

It is important to note that this cause of misalignment is structural rather than outcome-based. It reflects differences in the design of domestic regulations and legal culture, not disagreements over the acceptability of cross-border data transfers.

³²⁷ See *Agreement Establishing the African Continental Free Trade Area*, 2018 art 9.

³²⁸ See generally Graham Greenleaf & Bertil Cottier, “International and regional commitments in African data privacy laws: A comparative analysis” (2022) 44 *Computer Law & Security Review* 105638 at 5–8.

³²⁹ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* arts 20–22; *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 arts 4-12,16.

5.2.3 Institutional Asymmetry and Administrative Capacity

A third structural cause of CBDF misalignment comes from differences among domestic data protection authorities and related regulators. While the AfCFTA CBDF framework assumes the presence of competent authorities responsible for handling data protection and cross-border transfer rules, it does not define uniform institutional models, enforcement powers, or baseline resources.³³⁰

As a result, domestic authorities show significant variation in their ability to provide guidance, evaluate cross-border transfers, coordinate with foreign regulators, and offer consistent legal signals to market participants.³³¹ These differences influence how CBDF obligations are enforced in practice and lead to varying alignment outcomes, as shown in the institutional and implementation aspects of the Chapter 4 assessment.

The lack of a supranational supervisory body under the AfCFTA CBDF regime reinforces this asymmetry. Coordination and collaboration are expected, but enforcement and administration remain the responsibility of individual nations.³³² In such a governance arrangement, differences in institutional maturity are a predictable source of operational divergence.

5.2.4 Trade–Privacy Interface and Regulatory Orientation

A fourth structural cause of CBDF misalignment arises from the relationship between trade-focused CBDF commitments and local privacy and data protection laws. The AfCFTA CBDF framework is part of a trade agreement that emphasizes market integration, legal predictability,

³³⁰ *AfCFTA Digital Trade Protocol*, *supra* note 2 arts 20–21.

³³¹ Isaac Juma & Bukola Faturoti, “Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice” (2025) *International Review of Law, Computers & Technology* 1–26 at 18–20.

³³² The AfCFTA establishes intergovernmental cooperation and dispute settlement mechanisms but does not create a supranational supervisory or enforcement authority for CBDF governance. *Agreement Establishing the African Continental Free Trade Area*, 2018 art 30.

and cross-border operability.³³³ In contrast, domestic CBDF frameworks are mainly based on constitutional rights protection, administrative law, and sector-specific risk regulation.

This difference in regulatory focus creates structural tension. Trade-based CBDF obligations stress interoperability and a steady flow of data, while privacy-focused frameworks prioritize caution, accountability, and control over data movement. The AfCFTA CBDF framework addresses this tension with public policy exceptions and requirements for continuous safeguards rather than by placing domestic privacy regulations below trade liberalization.³³⁴ However, the lack of detailed reconciliation rules leaves significant interpretive room at the domestic level, which contributes to varying operational outcomes even without clear legal conflict.

5.2.5 Capacity Sensitivity and Multi-Level Normative Context

The final structural cause of CBDF misalignment comes from the capacity-sensitive design of the AfCFTA CBDF regime and its interaction with a multi-level normative environment. The Digital Trade Protocol acknowledges differences in development levels and institutional capacity among State Parties, stressing cooperation, technical assistance, and gradual implementation.³³⁵ This design choice affects implementation paths by allowing for different pacing and regulatory sequencing across jurisdictions.

Additionally, AfCFTA CBDF obligations work alongside existing regional and sub-regional normative frameworks, including those established within Regional Economic Communities. While AfCFTA commitments take precedence at the continental level, the existence of REC-level norms adds to legal layering and interpretive complexity at the local interface.³³⁶ Together, these

³³³ See the Preamble of *Agreement Establishing the African Continental Free Trade Area*, 2018.

³³⁴ *AfCFTA Digital Trade Protocol*, *supra* note 2 art 20(1)-(2), 22.

³³⁵ The preamble of the DTP explicitly recognises differing levels of development and digital readiness among State Parties and frames digital trade integration around cooperation and inclusiveness rather than immediate uniformity. See: *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade*.

³³⁶ See *Agreement Establishing the African Continental Free Trade Area*, 2018 art 5 and the Preamble of the Agreement.

factors shape alignment outcomes by placing CBDF implementation within a diverse and capacity-sensitive legal landscape.

5.3.0 Doctrinal Conflicts versus Capacity-Based Implementation Gaps

The structural sources of misalignment identified in Section 5.2 do not, by themselves, decide if the differences between domestic CBDF regimes and AfCFTA commitments lead to a legal violation. To make this determination, an additional analytical step must be taken to differentiate between divergence that shows doctrinal incompatibility with AfCFTA CBDF obligations and divergence that results from capacity limitations or differences in implementation within the AfCFTA legal framework.³³⁷ This distinction is crucial to prevent mixing up regulatory diversity with non-compliance and to maintain the legal integrity of the AfCFTA CBDF regime.³³⁸

5.3.1 Doctrinal Incompatibility under the AfCFTA CBDF Framework

Doctrinal incompatibility is when a domestic legal rule or practice undermines or significantly obstructs a core AfCFTA CBDF obligation. Under the Digital Trade Protocol and the Annex on Cross-Border Data Transfers, these obligations are laid out as rules that have specific exceptions.³³⁹ State Parties must allow cross-border data transfers for digital trade while maintaining the right to adopt measures that support legitimate public policy goals, such as

³³⁷ See generally: Mira Burri, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation” (2017) 51 UC Davis Law Review 65–133 at 82–86 Burri distinguishes legal incompatibility from regulatory implementation space in WTO law.

³³⁸ See generally: Alexander Beyleveld & Franziska Sucker, “Regulating Cross-Border Data Flows Under the AfCFTA Protocol on Digital Trade: The What, Why, How, Where, and When” (2023) SSRN Journal, online: <<https://www.ssrn.com/abstract=4437331>> at 14–35.

³³⁹ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* arts 20–24; *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 arts 23–26.

personal data protection, national security, and public order.³⁴⁰ These measures must also prevent arbitrary or disguised limitations on digital trade.³⁴¹

A domestic CBDF regime is doctrinally incompatible with AfCFTA commitments if it creates outright or effective bans on cross-border data transfers that are not covered by the recognized exceptions.³⁴² It is also incompatible if it imposes conditions that make cross-border operability feel impossible. Incompatibility may arise if domestic law does not uphold the personal data protection standards and continuity required by the CBDF Annex, which undermines the idea that data can flow across borders without reducing the protection for data subjects.³⁴³

Importantly, we assess doctrinal incompatibility based on legal effect, not just formal structure.³⁴⁴ Measures described in neutral or permissive language may still be incompatible if their combined effect systematically restricts cross-border data transfers beyond what the AfCFTA exceptions allow. On the other hand, having approval mechanisms, safeguards, or controls does not automatically mean there is incompatibility if these measures are justified under public policy exceptions in the Protocol and follow the related rules.³⁴⁵

5.3.2 Capacity-Based and Implementation-Driven Divergence

In contrast, capacity-based divergence happens when domestic CBDF regimes are formally aligned with AfCFTA obligations but differ in how they put those obligations into practice due to institutional, administrative, or technical limitations.³⁴⁶ This type of divergence is not about

³⁴⁰ *AfCFTA Digital Trade Protocol*, *supra* note 3 art 20(2); *Annex on Cross-Border Data Transfers*, *supra* note 3 arts 24–25.

³⁴¹ *AfCFTA Digital Trade Protocol*, *supra* note 3 art 20(2); *Annex on Cross-Border Data Transfers*, *supra* note 3 art 23(2).

³⁴² See generally: Burri, *supra* note 1 at 91–94.

³⁴³ *Annex on Cross-Border Data Transfers*, *supra* note 3 art 19(4), 21(c).

³⁴⁴ See generally P Delimatsis, “Determining the Necessity of Domestic Regulations in Services: The Best is Yet to Come” (2008) 19:2 *European Journal of International Law* 365–408 at 391.

³⁴⁵ See *Annex on Cross-Border Data Transfers*, *supra* note 3 arts 23–26.

³⁴⁶ See Delimatsis, “Determining the Necessity of Domestic Regulations in Services”, *supra* note 8 at 375–376.

rejecting AfCFTA rules but involves variations in regulatory techniques, administrative design, and the clarity or availability of guidance for implementation.³⁴⁷

As shown in the diagnostic assessment in Chapter 4, a large portion of the misalignment observed falls into this category.³⁴⁸ Domestic systems might use different combinations of delegated instruments, administrative discretion, or phased implementation approaches when dealing with cross-border data transfers. These differences affect the predictability and ease of compliance without legally prohibiting or contradicting AfCFTA CBDF obligations.

The AfCFTA CBDF framework allows for this kind of variation.³⁴⁹ While the CBDF Annex mandates that State Parties align their domestic data protection frameworks with the principles and standards outlined in the Annex, it does not require a uniform legal model, a single transfer mechanism, or identical institutional setups.³⁵⁰ Moreover, the Protocol encourages regulatory cooperation, technical support, and capacity-building, using language that promotes effort instead of pressing for immediate alignment in administrative capabilities.³⁵¹ Within this structure, varied implementation paths are a common aspect of early CBDF setup rather than clear evidence of a violation.³⁵²

³⁴⁷ See Mira Burri & Kholofelo Kugler, “Regulatory autonomy in digital trade agreements” (2024) 27:3 *Journal of International Economic Law* 397–423 at 403–405.

³⁴⁸ This assessment is derived from the author’s comparative diagnostic framework applied in Chapter 4 (Nigeria, Kenya, and South Africa), distinguishing doctrinal incompatibility from capacity-based divergence.

³⁴⁹ The AfCFTA recognizes principles such as flexibility, variable geometry, and special and differential treatment. See *Agreement Establishing the African Continental Free Trade Area*, 2018 art 5(c),(d).

³⁵⁰ See *Annex on Cross-Border Data Transfers*, *supra* note 3 art 16.

³⁵¹ *Ibid* arts 21–22.

³⁵² James Thuo Gathii, *African Regional Trade Agreements as Legal Regimes*, 1st edn (Cambridge: Cambridge University Press, 2011) Cambridge International Trade and Economic Law at 572.

5.3.3 The Legal Significance of the Distinction

The difference between doctrinal incompatibility and capacity-based divergence has clear legal implications under the AfCFTA CBDF regime.³⁵³ The Digital Trade Protocol and the CBDF Annex define cross-border data transfers for digital trade as the general rule while allowing exceptions only through specific public-policy reasons and with personal data protection safeguards in place.³⁵⁴ Within this rule and exceptions framework, divergence matters not because it simply exists, but because of how it impacts the obligations of the regime.

Doctrinal incompatibility happens when domestic CBDF measures undermine the legal framework of AfCFTA in one of three ways. First, incompatibility occurs when domestic laws or regulations deny the possibility of cross-border data transfers as the general rule, whether through outright bans or through burdensome requirements that make lawful transfers nearly impossible in practice.³⁵⁵ Second, incompatibility arises when restrictions on cross-border data transfers are put in place under public-policy goals but do not meet the criteria for recognized exceptions, including non-discrimination and avoiding arbitrary or disguised limits on digital trade.³⁵⁶ Third, incompatibility may occur when domestic rules allow cross-border transfers in theory but weaken the necessary personal data protection safeguards specified in the CBDF Annex, thus undermining the legal basis for cross-border operations.³⁵⁷

Divergence that does not meet these criteria, especially when it reflects different regulatory sequencing, administrative design, or institutional capacity, does not invalidate AfCFTA CBDF

³⁵³ See generally P Delimatsis, “Determining the Necessity of Domestic Regulations in Services: The Best is Yet to Come” (2008) 19:2 European Journal of International Law 365–408 at 373–377.

³⁵⁴ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* art 20; *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 art 24.

³⁵⁵ Mira Burri, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation” (2017) 51 UC Davis Law Review 65–133 at 97. Burri talks about the China - Audiovisual Products case where burdensome requirements adopted restricted foreign products. .

³⁵⁶ *Annex on Cross-Border Data Transfers*, *supra* note 2 art 23(2).

³⁵⁷ See *ibid* arts 4–11.

obligations in terms of treaty interpretation. Instead, it fits within the realm of managed divergence accepted by a regime that focuses on standard-based harmonization, regulatory cooperation, and implementation that considers capacity, without affecting the availability of formal dispute resolution mechanisms under the AfCFTA legal framework.

5.3.4 Implications for Alignment Assessment

Applying the above distinction clarifies the relevance of the alignment patterns seen in Chapter 4. While the case-study jurisdictions show different levels of alignment across various dimensions, the main sources of misalignment identified through the diagnostic methodology are operational rather than doctrinal.³⁵⁸ This finding directly stems from the framework and scoring rules described in Appendix A, which distinguish between legal structure and enforcement outcomes, avoiding simple compliance evaluations.

Recognizing the predominance of capacity-based divergence provides the basis for the alignment pathways explored in the next section. When misalignment is mainly operational, the appropriate legal response is to pursue regulatory cooperation, interpretive convergence, and institutional strengthening, while also keeping formal dispute resolution options available under the AfCFTA legal framework.³⁵⁹

5.4.0 Pathways for Operationalizing AfCFTA Obligations within Existing Domestic Framework

This section translates the Chapter 4 diagnostic findings into implementable pathways that do not depend on uniform domestic reform. The comparative analysis shows that the principal barriers to

³⁵⁸ This is derived from the author's diagnostic framework and evidence mapping in Chapter 4 and Appendix A, distinguishing doctrinal incompatibility from operational divergence.

³⁵⁹ *AfCFTA Digital Trade Protocol*, *supra* note 2 arts 42-43,45.

AfCFTA-consistent cross-border transfers are less often express statutory prohibitions than operational misalignment—including uneven guidance density, discretionary transfer administration, and institutional capacity gaps that undermine regulatory predictability. Operationalization should therefore prioritize mechanisms that: (i) preserve legitimate regulatory autonomy, while (ii) producing a minimum level of interoperability and predictable transfer conditions across State Parties.

The AfCFTA CBDF framework can support this approach through two complementary tracks: national-level operational alignment and continental-level coordination support. Both tracks remain bounded by the AfCFTA’s legal design, which facilitates transfers conditionally and preserves public-interest safeguards rather than imposing a single model of data governance.

5.4.1 National-Level Operational Alignment

At the national level, the AfCFTA CBDF regime can be implemented through interpretive and administrative alignment, rather than legislative convergence. First, State Parties should adopt a treaty-consistent interpretive approach that reads domestic cross-border transfer provisions, to the extent possible, in a manner that gives effect to AfCFTA-level obligations while preserving domestic privacy protections. This is not an invitation to dilute domestic safeguards; it is a method of reducing unnecessary friction where domestic law permits multiple plausible administrative interpretations.

Second, national regulators should calibrate transfer administration to reduce discretionary opacity. Where domestic systems rely on authorizations, approvals, or regulator-driven assessments, regulators should publish baseline criteria, standard decision timelines, and model documentation requirements for cross-border transfers. Chapter 4 shows that even where legal rules are broadly permissive, a lack of administratively legible criteria can generate de facto

barriers that are functionally equivalent to restriction. Publishing criteria does not eliminate discretion, but it disciplines it, thereby supporting AfCFTA-relevant predictability.

Third, domestic authorities should develop streamlined risk-based pathways for routine transfers related to ordinary digital trade operations (payment processing, fraud prevention, customer support, logistics), while reserving more stringent review for high-risk processing categories. This approach aligns with the AfCFTA benchmark's emphasis on conditional facilitation with safeguards: it reduces friction for low-risk commerce while preserving a defensible public-interest rationale for restrictions where necessary.³⁶⁰

5.4.2 Continental-Level Operational Support and Coordination

National implementation is supported by continental mechanisms outlined in the AfCFTA CBDF framework. The Annex on Cross-Border Data Transfers includes provisions for regulatory cooperation among relevant authorities, such as information sharing and mutual assistance, along with developing best practices.³⁶¹ These mechanisms encourage consistent interpretation and administration without establishing a supranational regulatory authority.³⁶²

One legally and institutionally feasible pathway is the development of non-binding but authoritative operational instruments, such as implementation guidelines, model clauses, and baseline documentation standards, which can be adopted through AfCFTA institutional processes.³⁶³ These instruments should be explicitly designed to address the types of misalignments diagnosed in Chapter 4, including, inconsistent transfer criteria, uneven transparency of administrative practice, and divergent regulator expectations regarding safeguards.

³⁶⁰ *Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade*, 2025 arts 20–21.

³⁶¹ *Ibid* art 21.

³⁶² *Ibid*.

³⁶³ African Union, *Guidelines for Integrating Data Provisions in Protocols on Digital Trade* (2023), online: <https://au.int/sites/default/files/documents/44807-doc-Guidelines-Integrating-Data-Digital-Trade-ENG-V3_161.pdf> at 36–37.

In addition, State Parties should institutionalise regulator-to-regulator cooperation focused on process alignment, rather than substantive harmonization.³⁶⁴ Cooperation should prioritise: (i) shared interpretive understandings of AfCFTA safeguards and exceptions; (ii) information-sharing on transfer risk assessment approaches; and (iii) capacity support arrangements for weaker enforcement institutions, since Chapter 4 shows that institutional asymmetry is a material driver of functional divergence even when statutory texts appear comparable.

These cooperative pathways are not costless. Regulators across African States operate under uneven staffing levels, technical expertise, and enforcement resources, creating asymmetries that can slow collective processes and strain sustained engagement.³⁶⁵ Coordination also entails non-trivial transaction and opportunity costs, including time diverted from domestic enforcement priorities and the need to reconcile divergent bureaucratic practices and regulatory cultures. In addition, sensitivity surrounding regulatory sovereignty limits the feasibility of binding supranational oversight and favours non-binding, process-oriented cooperation mechanisms. These constraints do not undermine the case for cooperation; rather, they explain why AfCFTA-based CBDF coordination must prioritise low-cost, incremental, and flexible instruments that discipline administrative practice without imposing unsustainable institutional burdens or requiring uniform domestic reform.³⁶⁶

³⁶⁴ See generally Kalypso Nicolaidis & Gregory Shaffer, “Transnational Mutual Recognition Regimes: Governance without Global Government” (2005) 68:3 *Law and Contemporary Problems* 263–318 at 289.

³⁶⁵ See generally *Regulating Data Protection and Cybersecurity in Africa: Findings from the Global Data Regulation Diagnostic*, by World Bank Group, in *Governance and the Digital Economy in Africa Technical Background Paper Series* (Washington, DC.: World Bank Group, 2023) at 11 online: <<https://openknowledge.worldbank.org/server/api/core/bitstreams/62e27761-1da1-467f-99a2-a6a1a3cf3b54/content>>.

³⁶⁶ *Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade* arts 42–43.

5.4.3 The Legal Limits of Operational Alignment

Operational alignment is not unlimited. Where domestic frameworks impose express localisation mandates, non-derogable sectoral retention rules, or binding prohibitions that cannot plausibly be reconciled with AfCFTA obligations and safeguards, interpretive alignment will not cure the conflict.³⁶⁷ In such cases, the AfCFTA legal order can provide a discipline through transparency obligations, structured justification, and cooperative engagement,³⁶⁸ but it cannot substitute for domestic legal change without exceeding the Protocol's design. Accordingly, the goal of the alignment pathways proposed here is not to eliminate all divergence, but to reduce unjustified and administratively generated friction and to ensure that restrictions are applied through defensible, transparent, and AfCFTA-consistent criteria.

5.5.0 Sequencing and Phasing of AfCFTA CBDF Implementation

The alignment pathways discussed in Section 5.4 function within an AfCFTA CBDF framework that does not require uniform procedures, institutional models, or transfer mechanisms. Although the AfCFTA Digital Trade Protocol establishes binding obligations for cross-border data transfers, the way those obligations are operationalized may vary across national legal systems, reflecting differences in institutional capacity and regulatory practice. However, any variation in implementation pace, must operate within the five-year period for legal alignment mandated by the Protocol after its coming into force.³⁶⁹

In this setting, sequencing and phasing should be understood as legally permissible modes of implementation within a fixed compliance horizon, rather than as staggered or deferred compliance with AfCFTA obligations.

³⁶⁷ *Annex on Cross-Border Data Transfers*, *supra* note 1 art 23(2).

³⁶⁸ *Ibid* arts 19, 26(4).

³⁶⁹ *AfCFTA Digital Trade Protocol*, *supra* note 7 art 48.

5.5.1 Legal Basis for Sequencing and Phasing of AfCFTA CBDF Implementation

The AfCFTA CBDF regime has a structure that includes rules along with exceptions. It considers permissibility as the norm while allowing states to pursue legitimate public policy goals, as long as they follow certain guidelines. Neither the Protocol nor the CBDF Annex requires a single administrative process, transfer method, or supervisory model, nor does it demand that all State Parties adopt the same implementation arrangements at the same time.³⁷⁰

This design is supported by provisions that acknowledge differences in development and institutional capability, emphasizing the importance of regulatory cooperation, technical assistance, and building capacity for implementation.³⁷¹ The use of "endeavor" language regarding institutional development and cooperation does not grant a legal right to delay compliance. Instead, it suggests a view where different implementation paths are allowed, as long as the essential obligations are upheld.

5.5.2 Sequencing as a Compliance-Permissible Implementation Practice

In this legal framework, sequencing acts as a compliance-permissible implementation practice instead of a strict doctrine of phased obligations. In practice, domestic implementation should focus on making sure that national frameworks do not create outright or effective bans on cross-border data transfers and that the basic safeguards outlined in the CBDF Annex are upheld. These factors capture the minimum legal requirements of AfCFTA CBDF obligations and help ensure that cross-border data flows for digital trade remain operational.

As institutional capacity improves, domestic authorities may refine administrative procedures, clarify regulatory guidance, and strengthen supervisory practices. Although these advancements increase legal certainty and regulatory effectiveness, they are not prerequisites for compliance if

³⁷⁰ *Ibid* arts 20–22; *Annex on Cross-Border Data Transfers*, *supra* note 1 art 24.

³⁷¹ See *AfCFTA Digital Trade Protocol*, *supra* note 7 art 48 and the Preamble.

the core permissive rule and safeguard continuity are already in place. This explanation does not set timelines or stages for implementation; it outlines a pattern of operationalization that aligns with the flexibility built into the AfCFTA CBDF framework.

5.5.3 Sequencing, Managed Divergence, and Alignment Assessment

Sequencing relates to the idea of managed divergence mentioned earlier in this chapter. When divergence is based on capacity rather than doctrine, differences in timing for implementation can clarify variations without suggesting legal inconsistency. A rigid assessment of alignment could misinterpret temporary administrative arrangements as non-compliance, especially in a system that relies on cooperation and standards-based harmonization instead of strict rules.

Acknowledging the time aspect of implementation does not weaken AfCFTA obligations. Rather, it clarifies how alignment should be evaluated by differentiating between structural incompatibility and transitional changes in regulatory approach or administrative development.

5.5.4 Legal Limits of Sequencing under AfCFTA Law

The acceptance of sequencing has clear legal boundaries. Temporal differentiation cannot be used to justify actions that contradict the general permissibility of cross-border data transfers, do not meet the guidelines for recognized public-policy exceptions, or threaten the ongoing personal data protection safeguards required by the CBDF Annex.³⁷² Additionally, sequencing cannot excuse ongoing regulatory delays where core obligations have yet to be implemented.³⁷³

If domestic measures go beyond these limits, the issue shifts from implementation method to legal inconsistency. In such cases, cooperative approaches do not replace access to formal compliance measures under AfCFTA law, including the option for dispute resolution according to the relevant AfCFTA provisions.

³⁷² *Ibid* art 48(3).

³⁷³ *Ibid* art 48(4).

5.5.5 Implications for Alignment Evaluation

Recognizing sequencing as a compliance-permissible practice sharpens the assessment of CBDF alignment. Rather than viewing divergence as a fixed state, the evaluation of alignment must consider whether domestic measures meet core AfCFTA obligations at a specific moment while moving toward greater operational coherence. This viewpoint aligns with the diagnostic methodology described in Chapter 4 and Appendix A, which distinguishes legal structure from enforcement results and avoids binary compliance conclusions.

By placing sequencing within the understanding of AfCFTA CBDF obligations, this section strengthens the main point of the chapter: effective integration of continental digital trade does not rely on immediate legal uniformity but on the organized, cooperative, and capacity-sensitive implementation of binding commitments.

5.6.0 Implications for Continental Digital Trade Integration

A central analytical implication of this thesis is that AfCFTA-relevant progress in cross-border data flows is more accurately assessed through legal interoperability than through formal uniformity. Chapter 4 demonstrates that domestic CBDF regimes can diverge in legislative form and regulatory technique while still being capable of producing AfCFTA-consistent outcomes, provided that transfer conditions are intelligible, safeguards are operationalized transparently, and administrative practice does not create unpredictable barriers. On this view, the integration function of the AfCFTA CBDF framework is not to replace domestic privacy regimes, but to structure a predictable legal environment for cross-border digital trade under treaty-based conditions and exceptions.³⁷⁴

³⁷⁴ See the Preamble to *AfCFTA Digital Trade Protocol*, *supra* note 7.

Accordingly, the appropriate benchmark for integration is whether firms and regulators can anticipate, with reasonable certainty, the conditions under which cross-border transfers occur and the safeguards that may justify restriction. Where domestic law provides multiple transfer pathways but fails to operationalize them through clear criteria, interoperability weakens even in the absence of formal prohibitions. AfCFTA implementation should therefore prioritize the reduction of uncertainty and administrative opacity as integration obstacles.

Alignment matters not only as a compliance question but as a trust-building mechanism. Predictable transfer criteria and disciplined invocation of exceptions reduce perceived regulatory risk for digital traders and facilitate routine cross-border processing. Conversely, where domestic institutions have limited enforcement credibility or inconsistent administrative practice, cross-border transfers may become commercially unattractive even if formally lawful. This reinforces the Chapter 4 finding that institutional capacity asymmetry is an integration constraint that legal drafting alone cannot resolve.

Given the AfCFTA's current institutional design, integration should be pursued through cooperative mechanisms that converge processes rather than laws.³⁷⁵ The AfCFTA CBDF framework is best understood as enabling structured coordination: shared operational standards, regulator cooperation, and capacity support that collectively reduce friction while leaving domestic systems intact. This is a legally and politically realistic pathway that matches the conditional facilitation logic of the CBDF regime.

Finally, integration requires a credible approach to managed divergence. Not all domestic variation undermines AfCFTA objectives. Divergence becomes problematic when it produces unjustified barriers, unpredictable administration, or restrictions that cannot be defended under treaty-based

³⁷⁵ *Ibid* arts 42–43.

safeguards.³⁷⁶ A sustainable AfCFTA approach should therefore distinguish (i) divergence that remains compatible because it is transparent, justified, and safeguard-based, from (ii) divergence that functions as disguised restriction or administrative obstruction. This distinction provides a disciplined basis for future AfCFTA monitoring and iterative implementation without reverting to unrealistic harmonization claims.

5.7.0 Conclusion

This chapter has explored how the AfCFTA CBDF regime might work in practice, considering the differences observed domestically. Using the legal standard set in Chapter 3 and the assessment from Chapter 4, this chapter argues that most of the misalignments found in the case-study jurisdictions do not usually stem from doctrinal conflicts with AfCFTA obligations. Instead, as shown in the comparative findings and scorecard analysis, misalignment often results from differences in institutional capacity, regulatory methods, and the sequence of implementation across various areas.

By separating doctrinal conflicts from capacity-related differences, this chapter clarifies the legal importance of regulatory variation within the AfCFTA CBDF framework. This separation provides an interpretive threshold, based on the structure of the Digital Trade Protocol and the CBDF Annex, for determining when domestic CBDF measures violate AfCFTA commitments and when they remain within the tolerated space of managed divergence.

The analysis also shows that AfCFTA law does not require uniform legal alignment for continental digital trade integration. Instead, this chapter identifies ways to implement compliance that are built into the AfCFTA CBDF framework itself, such as treaty-consistent interpretation,

³⁷⁶ *Annex on Cross-Border Data Transfers*, *supra* note 1 arts 23–24.

administrative adjustments, regulatory cooperation, and capacity-sensitive sequencing. These methods do not suggest policy changes or reforms; instead, they describe legally acceptable ways to implement binding CBDF obligations across various domestic legal systems. At the same time, this chapter highlights that such flexibility has clear legal boundaries. Operational alignment cannot justify measures that violate the general rules on cross-border data transfers, avoid the requirements linked to recognized public policy exceptions, or weaken personal data protection safeguards outlined in the CBDF Annex.

Overall, this analysis positions the AfCFTA CBDF regime as a framework focused on legal interoperability rather than strict uniformity. Effective continental digital trade integration relies on cooperation and sensitive handling of binding treaty obligations across different regulatory environments. This integration is supported by coordination mechanisms and backed by enforceable legal commitments. When divergence becomes a matter of doctrinal conflict, cooperative alignment methods are not enough, and the availability of formal compliance tools, including dispute resolution, under the AfCFTA legal framework remains essential.

The next General Conclusion places these findings within the larger goals of the thesis, reflects on their contribution to the study of digital trade integration and cross-border data flows in Africa, and outlines the limits and implications of this study's analytical approach.

General Conclusion

This thesis examined the governance of cross-border data flows (CBDF) under the AfCFTA Digital Trade Protocol and its Annex on Cross-Border Data Transfers. It particularly focused on how domestic CBDF regimes in Nigeria, Kenya, and South Africa vary from or align with the emerging continental framework. Addressing concerns in the literature that regulatory fragmentation could harm Africa's digital trade integration, the thesis viewed CBDF governance as a matter of legal coordination rather than a failure to achieve uniformity. It looked at not just whether domestic regimes differ, but when and how such differences matter under AfCFTA law. The analysis unfolded in three stages. First, the thesis created a framework to assess CBDF alignment across five areas: legal-normative foundations, regulatory scope, institutional mechanisms, rights and digital safeguards, and socio-economic and technical context. Second, it defined the AfCFTA CBDF regime as a legal standard, interpreting the Digital Trade Protocol and the CBDF Annex as a system that allows cross-border data transfers for digital trade under conditions of safeguard continuity and controlled public-policy exceptions. Third, it applied this standard to the domestic CBDF regimes of Nigeria, Kenya, and South Africa, using a structured approach to evaluate alignment and misalignment across the identified areas.

Based on this analysis, the thesis makes three main contributions. First, it questions the tendency in existing scholarship to mix regulatory diversity with legal incompatibility. Using the comparative findings in Chapter 4, the thesis argues that the primary types of misalignment observed across the case studies stem more from differences in institutional capacity, regulatory methods, and implementation timing than from direct conflict with AfCFTA CBDF obligations. By separating doctrinal incompatibility from capacity-based differences, the thesis establishes a threshold—rooted in the structure of the Protocol and Annex—for determining when domestic

CBDF measures undermine AfCFTA commitments versus when they fall within acceptable, managed differences allowed by a standards-based trade regime.

Second, the thesis reframes continental digital trade integration under the AfCFTA in terms of legal interoperability instead of uniformity. It suggests that the AfCFTA CBDF regime does not require identical domestic laws or a supranational regulatory body for integration. Rather, integration occurs when domestic legal systems can effectively work together to enable predictable cross-border data flows under shared rules regarding permissibility, safeguard continuity, and specific exceptions. This perspective is in line with the AfCFTA's institutional design and avoids unrealistic demands for immediate uniform legal harmonization among diverse states.

Third, the thesis offers a practical explanation of how AfCFTA CBDF obligations can be implemented. It identifies consistent methods of implementation, such as treaty-consistent interpretation, administrative adjustment, regulatory collaboration, and capacity-sensitive sequencing, that allow compliance within existing legal systems. This explanation does not overlook the Protocol's clear requirement for State Parties to align domestic laws within the designated period after the agreement goes into effect, nor does it imply that legislative change is unnecessary. Instead, it clarifies that alignment does not always mean an immediate complete legal overhaul or strict uniformity. It shows that AfCFTA law allows for gradual implementation that aligns with existing legal reforms. At the same time, the thesis emphasizes the legal limits of flexibility: operational alignment cannot justify measures that contradict the permissibility of cross-border data transfers, evade exception discipline, or weaken personal data protection safeguards.

Several implications arise from these findings. For AfCFTA CBDF governance, the analysis indicates that integration efforts should focus on legal interoperability, regulatory cooperation, and

capacity-building rather than on premature or formal harmonization. For domestic regulators, it highlights that compliance with AfCFTA CBDF obligations is not simply yes or no; it depends on legally sound implementation choices that honor both treaty commitments and domestic realities. For the digital trade literature, the thesis provides an Africa-specific perspective on CBDF governance, resisting the replication of external adequacy models and overly lenient approaches that minimize the importance of safeguards and legal discipline.

The thesis also has notable limitations. Its focus on three jurisdictions does not reflect the full range of African CBDF regimes. Its analytical framework and scoring methods involve interpretive decisions, especially in differentiating doctrinal incompatibility from capacity-based divergence. Additionally, the analysis emphasizes law on paper and institutional design rather than law in practice and does not examine the economic consequences of CBDF alignment or misalignment. Lastly, as the AfCFTA CBDF regime develops through ratification, domestic alignment, and possible dispute resolution practices, future changes may refine or question some of the interpretive conclusions made here.

Future research could expand this framework to more jurisdictions, explore how AfCFTA CBDF rules interact with regional economic community instruments, or investigate how new AfCFTA dispute settlement practices clarify the legal thresholds highlighted in this study. As digital trade grows across the continent, the legal governance of cross-border data flows will remain crucial for Africa's integration into the global digital economy.

In conclusion, this thesis contends that the AfCFTA CBDF regime should be seen not as an effort for uniform legal harmonization, but as a framework for managing regulatory diversity through legally disciplined interoperability. If properly implemented, the AfCFTA has the potential to

facilitate meaningful continental digital trade integration while respecting regulatory autonomy and protecting fundamental data protection interests.

Bibliography

Primary Materials

International Treaties

- African Union Convention on Cybersecurity and Personal Data Protection, 2014.
- Agreement Establishing the African Continental Free Trade Area, 2018.
- Annex on Cross-Border Data Transfers to the African Continental Free Trade Area Protocol on Digital Trade, 2025.
- Compiled Annexes to the African Continental Trade Area Protocol on Digital Trade, 2025.
- Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade.

Legislations: Kenya

- Data Protection (Civil Registration) Regulations, Legal Notice No 196 of 2020, 2020.
- Data Protection (Registration of Data Controllers and Data Processors) Regulations, Legal Notice No 265 of 2021, 2021.
- The Data Protection Act, 2019.
- The Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.
- The Data Protection (General) Regulations, 2021.

Legislation: Nigeria

- Central Bank of Nigeria Guidelines on Point of Sale (POS) Card Acceptance Services.
- Designation and Protection of Critical National Infrastructure, 2024.
- Nigerian Data Protection Act, 2023.
- Nigerian Communications Act.

- Regulatory Framework for Bank Verification Number (Operations) and watch-list for the Nigerian banking industry, 2021.
- The Constitution of the Federal Republic of Nigeria, 1999 (as amended) through 2011.

Legislation: South Africa

- Cybercrimes Act, Act No 19 of 2020.
- National Cybersecurity Policy Framework of 2015.
- Protection of Personal Information Act (POPI Act) 2013, 2013.
- Regulations Relating to the Protection of Personal Information 2018.
- Regulations Relating to the Protection of Personal Information 2025, 2025.

Secondary Sources

Other Materials

- African Union, *African Union Data Policy Framework* (2022), online: <https://au.int/en/documents/20220728/au-data-policy-framework>.

Secondary Materials: Conference Papers and Presentations

- Director General, Annual Report by the Director-General of the WTO (Mid-October 2022 - Mid-October 2023) (2024), online: <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/TPR/OV26.pdf&Open=True>.
- Ekpo, Otuekong, Abasifiok Okokon & Monday Akpakpan, *Data Protection in the Digital Age: A Comparative Analysis of Nigeria's NDPA and the EU's GDPR*. (New York, NY, USA: Association for Computing Machinery, 2025).
- Gao, Henry, *Data Sovereignty and Trade Agreements: Nailing Jello to the Wall?* (2021).

- Martin, Nicholas & Frank Ebbers, *When Regulatory Power and Industrial Ambitions Collide: The “Brussels Effect,” Lead Markets, and the GDPR*, Stefan Schiffner, Sebastien Ziegler & Adrian Quesada Rodriguez, eds (Cham: Springer International Publishing, 2022).

Secondary Materials: Book Sections

- Aaronson, Susan Ariel, “Data Is Different, So Policymakers Should Pay Close Attention to Its Governance” in Mira Burri, ed, *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021) 340.
- Babalola, Olumide, “Data Protection Legal Regime and Data Governance in Africa: An Overview” in Bitange Ndemo et al, eds, *Data Governance and Policy in Africa* (Cham: Springer International Publishing, 2023) 71.
- Bon, Anna, Francis Saa-Dittoh & Hans Akkermans, “Bridging the Digital Divide” in Hannes Werthner et al, eds, *Introduction to Digital Humanism: A Textbook* (Cham: Springer Nature Switzerland, 2024) 283.
- Burri, Mira, “Data Flows and Global Trade Law” in Mira Burri, ed, *Big Data and Global Trade Law*, 1st edn (Cambridge University Press, 2021) 11.
- Burri, Mira, “Introduction” in Mira Burri, ed, *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021) 1.
- Das, Sujitesh, “Flattening the Diversified Sphere through Digital Inclusivity” in Kakoli Sen & Sujata Shahi, eds, *Creating a Culture of Diversity and Inclusiveness in India Inc: Practitioners Speak* (Singapore: Springer, 2021) 87.
- Ferracane, Martina F, “The Costs of Data Protectionism” in Mira Burri, ed, *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021) 63.

- Jackson, John H, ed, “Challenges to fundamental assumptions of international law” in *Sovereignty, the WTO, and Changing Fundamentals of International Law* Hersch Lauterpacht Memorial Lectures (Cambridge: Cambridge University Press, 2006) 1.
- Maily Fidler, “African Data Protection Laws: Politics, But as Usual” in Patricia Boshe, Moritz Hennemann & Ricarda von Meding, eds, *African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward* Global Privacy Law Review (2022).
- Oloni, Victoria, “Cross-Border Data Flows: Oiling the Wheel of the African Digital Economy” in Raymond Atuguba Akongburo et al, eds, *African Data Protection Laws: Regulation, Policy, and Practice* (De Gruyter, 2024) 157.
- Sucker, Franziska & Alexander Beyleveld, “African rules on cross-border data flows: The significance of regulatory convergence and the AfCFTA Digital Trade Protocol’s potential contribution” in *Comparative Data Law* MPI Studies on Intellectual Property and Competition Law (Switzerland: Springer Nature Switzerland, 2024).
- Trachtman, Joel P, “The Future of International Law: Global Government” in Joel P Trachtman, ed, *The Future of International Law: Global Government* ASIL Studies in International Legal Theory (Cambridge: Cambridge University Press, 2013)

Secondary Materials: Electronic Sources

- Abuja, Vincent Ikuomola, “ECOWAS plans amendments of supplementary act — Kalu” (18 August 2024), online: *The Nation Newspaper* <<https://thenationonlineng.net/ecowas-plans-amendments-of-supplementary-act-kalu/>>.

- Aly Apacible-Bernardo & Kayla Bushey, “Data protection and privacy laws now in effect in 144 countries | IAPP” (23 October 2025), online: *IAPP* <https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries?utm_source=chatgpt.com>.
- Arindrajit Basu, “Can the WTO build consensus on digital trade?” (1 August 2025), online: *Hinrich Foundation* <<https://www.hinrichfoundation.com/research/article/digital/can-the-wto-build-consensus-on-digital-trade/>>.
- Bilateralsorg, “AfCFTA digital trade protocol: Unveiling critical flaws” (2024), online: *Bilaterals.org* <<https://www.bilaterals.org/?afcfta-digital-trade-protocol-50237>>.
- Burri, Mira, “How Should the WTO Respond to the Data-driven Economy?” (21 December 2024), online: *Centre for International Governance Innovation* <<https://www.cigionline.org/articles/how-should-wto-respond-data-driven-economy/>>.
- CIPIT, “Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa” (23 November 2023), online: *Centre for Intellectual Property and Information Technology Law* <<https://cipit.org/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/>>.
- Ceretto, Ludovica et al, “EU-Japan deal on data flows enters into force: A New Era of Digital Economic Cooperation” (17 October 2024), online: *RPLT RP legalitax* <<https://www.rplt.it/eu-japan-deal-on-data-flows-enters-into-force-a-new-era-of-digital-economic-cooperation/>>.
- Dan Allan Kipkoech, “Navigating the Crossroads: The Challenges of Cross-Border Data Flows under Domestic Laws in Africa” (23 November 2023), online: *Centre for Intellectual Property and Information Technology Law* <<https://cipit.org/navigating-the-crossroads-the-challenges-of-cross-border-data-flows-under-domestic-laws-in-africa/>>.

- Dharshini Prasad, “Regional integration and the African Continental Free Trade Agreement: From Parallelism to Harmonisation” (2021), online: *International Bar Association* <<https://www.ibanet.org/regional-integration-afcfta>>.
- Digital Watch Observatory, “Draft of digital trade protocol to AfCFTA circulated” (21 February 2024), online: *Digital Watch Observatory* <<https://dig.watch/updates/draft-of-digital-trade-protocol-to-afcfta-circulated>>.
- Donrich Thaladar, “Harmonizing Africa’s Data Governance: Challenges and Solutions” (2023), online: *Bill of Health* <<https://blog.petrieflom.law.harvard.edu/2023/11/06/harmonizing-africas-data-governance-challenges-and-solutions/>>.
- Ezike, Eberechukwu, Ayomide Abiodun & Mojinyinoluwa Adegboye, “Cross-Border Data Transfers: Tackling Compliance Challenges in Africa’s Digital Economy” (14 July 2025), online: *The Gravitas Review of Business & Property Law* <<https://gravitasreview.com.ng/product/cross-border-data-transfers-compliance-challenges-africas-digital-economy/>>.
- Florence Jaumotte et al, “How Pandemic Accelerated Digital Transformation in Advanced Economies” (21 March 2023), online: *IMF* <<https://www.imf.org/en/Blogs/Articles/2023/03/21/how-pandemic-accelerated-digital-transformation-in-advanced-economies>>.
- ITIF, “Nigeria’s Cross-Border Data Transfer Regulation” (9 June 2025), online: *Information Technology and Innovation Foundation* <<https://itif.org/publications/2025/06/09/nigeria-cross-border-data-transfer-regulation/#>>.

- Margaret Speigelman, *UNCTAD chief: Multilateral trade system must be made more inclusive* | *InsideTrade.com* (2024).
- Miracle Okoro, “African Union Adopts Critical Annexes to AfCFTA Digital Trade Protocol: Opportunities in Africa’s Digital Trade Ecosystem - CLG Global” (1 April 2025), online (Law firm): *CLG* <<https://clgglobal.com/african-union-adopts-critical-annexes-to-afcfta-digital-trade-protocol-opportunities-in-africas-digital-trade-ecosystem/>>.
- Stuart, John, “The AfCFTA Digital Trade Protocol – clarification of key issues”, online: *Tralac Blog* <<https://www.tralac.org/documents/blogs/5292-tralac-blog-stuart-the-afcfta-digital-trade-protocol-clarification-of-key-issues-25022024/file.html>>.
- WTO, *Electronic commerce Gateway - Briefing Note*.
- ———, “Work Programme on E-Commerce” (16 July 2025), online: *WTO* <https://www.wto.org/english/tratop_e/ecom_e/ecom_work_programme_e.htm>.

Secondary Sources: Journal Articles

- Aaronson, Susan, “Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security” (2015) 14:4 *World Trade Review* 671–700.
- Aaronson, Susan Ariel, “Data Is a Development Issue” (2019) 223 *CIGI Papers*, online: <<https://www.cigionline.org/static/documents/documents/paper%20no.223.pdf>>.
- Aaronson, Susan Ariel, “Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows” (2018) 197 *CIGI Papers*.
- Aaronson, Susan Ariel & Patrick Leblond, “Another Digital Divide: The Rise of Data Realms and its Implications for the WTO” (2018) 21:2 *Journal of International Economic Law* 245–272.

- Abendin, Simon & Pingfang Duan, “International trade and economic growth in Africa: The role of the digital economy” (2021) 9:1 Cogent Economics & Finance 1911767.
- Abraham, Rene, Johannes Schneider & Jan vom Brocke, “Data governance: A conceptual framework, structured review, and research agenda” (2019) 49 International Journal of Information Management 424–438.
- Ademuyiwa, Idris & Adedeji Adeniran, “Assessing Digitalization and Data Governance Issues in Africa” (2020) 244 CIGI Papers, online: <<https://www.econstor.eu/handle/10419/299716>>.
- Ahmed, Usman, “The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade” (2019) 18:S1 World Trade Review S99–S120.
- Alhassan, Ibrahim, Sammon ,David & Mary Daly, “Data governance activities: an analysis of the literature” (2016) 25:sup1 Journal of Decision Systems 64–75.
- Andrew Osehi Enaifoghe, “South Africa’s Politics of Regional Integration in SADC and its Socio-economic Implications” (2019) 6:1 Journal of African Foreign Affairs 85–106.
- Asif Khan, “The Intersection of Artificial Intelligence and International Trade Laws: Challenges and Opportunities” (2024) 32:1 IIUM Law Journal 103–152.
- Azmeh, Shamel, Christopher Foster & Jaime Echavarri, “The International Trade Regime and the Quest for Free Digital Trade” (2020) 22:3 Int Stud Rev 671–692.
- Babalola, Olumide, “Transborder flow of personal data (TDF) in Africa: Stocktaking the ills and gains of a divergently regulated business mechanism” (2024) 52 Computer Law & Security Review 105940.
- Badran, Mona Farid, “Economic impact of data localization in five selected African countries” (2018) 20:4 Digital Policy, Regulation and Governance 337–357.

- Bazzanella, Sandro & Jean-François Le Bihan, “Support for Harmonization of ICT Policies in Sub-Sahara Africa”.
- Beyleveld, Alexander & Franziska Sucker, “Regulating Cross-Border Data Flows Under the AfCFTA Protocol on Digital Trade: The What, Why, How, Where, and When” (2023) SSRN Journal, online: <<https://www.ssrn.com/abstract=4437331>>.
- Brian Daigle, “Data Protection Laws in Africa: A Pan- African Survey and Noted Trends” (2021) *Journal of International Commerce and Economics* 1–27.
- Bryant, Justin, “Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights” (2021) 24:2 *Stan Tech L Rev* 382-.
- Burri, Mira, “Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions: Implications for the Future EU-ASEAN Agreement” (2022) 49 *Legal Issues of Economic Integration* 149–168.
- Burri, Mira, “The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation” (2017) 51 *UC Davis Law Review* 65–133.
- Burri, Mira, “The Impact of Digitalization on Global Trade Law” (2023) 24 *German Law Journal* 551–573.
- Burri, Mira, “The International Economic Law Framework for Digital Trade” (2015) 135 *Zeitschrift für Schweizerisches Recht* 10–72.
- Burri, Mira, “The Regulation of Data Flows Through Trade Agreements” (2017) 48 *Georgetown Journal of International Law* 407.
- Burri, Mira, “Towards a New Treaty on Digital Trade” (2021) 55:1 *Journal of World Trade* 77–100.

- Burri, Mira, “Trade Law 4.0: Are We There Yet?” (2023) 26:1 *Journal of international economic law* 90–100.
- Burri, Mira & Kholofelo Kugler, “Regulatory autonomy in digital trade agreements” (2024) 27:3 *Journal of International Economic Law* 397–423.
- Burri, Mira & Rodrigo Polanco, “Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset” (2020) 23:1 *J Int Economic Law* 187–220.
- Burri, Mira, María Vásquez Callo-Müller & Kholofelo Kugler, “The Evolution of Digital Trade Law: Insights from TAPED” (2024) 23:2 *World Trade Review* 190–207.
- Calzati, Stefano, “‘Data sovereignty’ or ‘Data colonialism’? Exploring the Chinese involvement in Africa’s ICTs: a document review on Kenya” (2022) 40:2 *Journal of Contemporary African Studies* 270–285.
- Chaisse, Julien, “‘The Black Pit:’ Power and Pitfalls of Digital FDI and Cross-Border Data Flows” (2023) 22:1 *World Trade Review* 73–89.
- Chander, Anupam & Uyãn P Lã, “Data Nationalism” (2015) 64:3 *Emory Law Journal* 678–739.
- Chander, Anupam & Paul Schwartz, “Privacy and/or Trade” (2023) 90:1 *U Chi L Rev* 49–136.
- Chen, Si, “China’s Path to Regulatory Harmonization of Cross-Border Data Flows” (2025) 22:4 *US-China L Rev* 198–204.
- Chowdhury, Tanveer Ehsan Chowdhury Tanveer Ehsan et al, “From Crisis to Opportunity: How Covid-19 Accelerated the Global Shift to Online Business” (2022) 3:1 *Pathfinder of Research* 18–18.

- Christopher Kuner, “Reality and Illusion in EU Data Transfer Regulation Post Schrems” (2017) 18:4 German Law Journal 881–918.
- CN Dumle, “An assessment of Development Mechanism in Africa: Abuja Treaty/African Economic Community (AEC), 1991-2000” (2023) 3:4 Niger Delta Journal of Gender, Peace & Conflict Studies 339–351.
- Coetzee, Juana, “Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 - Part II: The Data Transfer Provision” (2024) 27 Potchefstroom Elec LJ 1–29.
- Curtiss, Tiffany, “Privacy Harmonization and the Developing World: The Impact of the EU’s General Data Protection Regulation on Developing Economies”.
- Daniel Castrol & Ellyse Dick, “The Role and Value of Standard Contractual Clauses in EU-U.S. Digital Trade” (2020) Information Technology and Innovation Foundation, online: <https://itif.org/publications/2020/12/17/role-and-value-standard-contractual-clauses-eu-us-digital-trade/>.
- Deane, Felicity et al, “Trade in the Digital Age: Agreements to Mitigate Fragmentation” (2024) 14:1 Asian journal of international law (Cambridge, UK) 154–179.
- Delimatsis, P, “Determining the Necessity of Domestic Regulations in Services: The Best is Yet to Come” (2008) 19:2 European Journal of International Law 365–408.
- Delimatsis, Panos, “Global Trade-Enabling Law” (2021) 13 Indian Journal of International Economic Law, online: <https://papers.ssrn.com/abstract=4029104>.
- Echandi, Roberto, Maryla Maliszewska & Victor Steenbergen, “Making the Most of the African Continental Free Trade Area” (2022) World Bank Publications - Books, online: <https://ideas.repec.org/b/wbk/wbpubs/37623.html>.

- Fenwick, Mark, Wulf A Kaal & Erik P M Vermeulen, “Regulation Tomorrow: What Happens When Technology Is Faster than the Law” (2016) 6 Am U Bus L Rev 561.
- Ferencz, Janos, “The OECD Digital Services Trade Restrictiveness Index” (2019) 221 OECD Trade Policy Papers (OECD Trade Policy Papers) , online: <<https://ideas.repec.org/p/oec/traaab/221-en.html>>.
- Ferracane, Martina F, Simón González Ugarte & Erik Van Der Marel, “The Brussels effect in Africa: is it beneficial for intra-regional trade in digital services?” (2025) 28:1 Journal of International Economic Law 1–22.
- Floridi, Luciano, “Soft ethics, the governance of the digital and the General Data Protection Regulation” (2018) Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, online: <<https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0081>>.
- Foster, Christopher, “The Digital Trade Agenda and Africa” (2018) Bridges Africa, online: <https://www.academia.edu/38097178/The_Digital_Trade_Agenda_and_Africa>.
- Francesca Casalini & Javier López González, “Trade and Cross-Border Data Flows” (2019) 220 OECD Trade Policy Papers (OECD Trade Policy Papers) , online: <https://www.oecd.org/en/publications/trade-and-cross-border-data-flows_b2023a47-en.html>.
- Francesca Casalini, Javier López-González, & Taku Nemoto, “Mapping commonalities in regulatory approaches to cross-border data transfers” (2021) 248 OECD Trade Policy Papers, online: <https://www.oecd.org/en/publications/mapping-commonalities-in-regulatory-approaches-to-cross-border-data-transfers_ca9f974e-en.html>.

- Frank J Schweitzer, Ian Saccomanno, & Naoto Nelson Saika, “The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade—Part I” (2024) 1:2 *The Global Trade Law Journal* 103–118.
- Gao, Henry S, “Data Sovereignty and Trade Agreements: Three Digital Kingdoms” (2021) SSRN Journal, online: <<https://www.ssrn.com/abstract=3940508>>.
- Gao, Raymond Yang, “A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows” (2023) 22:4 *Chinese Journal of International Law* 707–787.
- Greenleaf, Graham, “G20 Makes Declaration of ‘Data Free Flow With Trust’: Support and Dissent” (2019) 160 *Privacy Laws & Business International Report* 189–19.
- Greenleaf, Graham, “Global Data Privacy Laws 2019: 132 National Laws & Many Bills” (2019) 156 *Privacy Laws & Business International Report* 14–18.
- Greenleaf, Graham & Bertil Cottier, “Comparing African Data Privacy Laws: International, African and Regional Commitments” (2020) 32 SSRN Journal, online: <<https://www.ssrn.com/abstract=3582478>>.
- Greenleaf, Graham & Bertil Cottier, “International and regional commitments in African data privacy laws: A comparative analysis” (2022) 44 *Computer Law & Security Review* 105638.
- Gunasekara, Gehan, “The “Final” Privacy Frontier? Regulating Trans-Border Data Flows” (2009) 17:2 *Int J Law Info Tech* 147–179.

- Hoofnagle, Chris Jay, van der Sloot ,Bart & Frederik Zuiderveen and Borgesius, “The European Union general data protection regulation: what it is and what it means**” (2019) 28:1 Information & Communications Technology Law 65–98.
- Janos Ferencz, Javier López-González, & Irene Oliván García, “Artificial Intelligence and International Trade: Some Preliminary Implications” (2022) 260 OECD Trade Policy Papers.
- Jennifer Daskal & Justin Sherman, “Data Nationalism on the Rise: The Global Push for State Control of Data” (2020) Economic Impact and Feasibility of Data Dividends.
- Joshua P Meltzer, “Governing Digital Trade” (2019) 18:S1 World trade review S23–S48.
- Juma, Isaac & Bukola Faturoti, “Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice” (2025) International Review of Law, Computers & Technology 1–26.
- Kaddu, Sarah & Francis Ssekitto, “Africa’s Data Privacy Puzzle: Data Privacy Laws and Compliance in Selected African Countries” (2023) 18:2 University of Dar es Salaam Library Journal, online: <<https://www.ajol.info/index.php/udslj/article/view/264002>>.
- Kaya Mehmet & Shahid Hamza, “Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance” (2025) 4:2 Interdisciplinary Studies in Society, Law, and Politics 219–233.
- Kere, Safilidin & Amara Zongo, “Digital technologies and intra-African trade” (2023) 173 International Economics 359–383.
- King’ori, Mercy, “Cross-Border Data Flows in Africa: Examining Policy Approaches and Pathways to Regulatory Interoperability” (2024) June Issue Future of Privacy Forum,

online: <<https://fpf.org/wp-content/uploads/2025/06/June-Issue-Brief-Cross-Border-Data-Flows-in-Africa.pdf>>.

- Kola Odeku & Teron Rikhotso, “African Continental Free Trade Area (AfCFTA): An Impetus for Intra-African Trade Integration” 10:1 Journal of African Foreign Affairs, online: <<https://journals.co.za/doi/10.31920/2056-5658/2023/v10n1a6>>.
- Koops, Bert-Jaap, “The trouble with European data protection law” (2014) 4:4 International Data Privacy Law 250–261.
- Kristina Irion, Margot E Kaminski, & Svetlana Yakovleva, “Privacy Peg, Trade Hole: Why We (Still) Shouldn’t Put Data Privacy in Trade Law” The University of Chicago Law Review, online: <<https://lawreview.uchicago.edu/online-archive/privacy-peg-trade-hole-why-we-still-shouldnt-put-data-privacy-trade-law>>.
- Kuner, Christopher, “Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future” (2010) TILT Law & Technology Working Paper No 016/2010, online: <<https://papers.ssrn.com/abstract=1689483>>.
- Labadie, Clément & Christine Legner, “Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR”.
- Laibuta, Mugambi, “The Evolution of Privacy and Data Protection in Kenya” (2024) 30:1 Fundamina : A Journal of Legal History 116–165.
- Leblond, Patrick & Susan Ariel Aaronson, “A Plurilateral “Single Data Area” Is the Solution to Canada’s Data Trilemma” (2019) 226.
- Lemma, Alberto, Max Mendez-Parra & Laura Naliaka, “The AfCFTA: unlocking the potential of the digital economy in Africa”.

- LeSieur, François, “Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy” (2012) 2:2 International Data Privacy Law 93–104.
- López Jiménez, Daniel Fernando & Juan Pablo del Alcázar Ponce, “Digital Transformation in Ecuador COVID-19 Pandemic as an accelerator to E-Commerce” (2022) 11:22 Communication Papers: Media Literacy and Gender Studies 83–94.
- Makulilo, A B, “Data Protection Regimes in Africa: too far from the European “adequacy” standard?” (2013) 3:1 International Data Privacy Law 42–50.
- Makulilo, Alex B, “Myth and reality of harmonisation of data privacy policies in Africa” (2015) 31:1 Computer Law & Security Review 78–89.
- Manfred Kouty, “Boosting the intra-African digital trade in the AfCFTA context: does regulatory framework matter?” (2024) 2:1 DESD 1–15.
- Mannion, Cara, “Data Imperialism: The GDPR’s Disastrous Impact on Africa’s E-Commerce Markets Notes” (2020) 53:2 Vand J Transnat’l L 685–712.
- Manyika, James & Charles Roxburgh, “The growth of the Internet has significantly transformed the modern economy.1 The Internet contributes to higher productivities and lower trading costs in traditional industries.2 More importantly, it provides a platform for a widening array of emerging industries, including cloud computing,3 the Internet of Things (IoT),4 big data,5 social media,6 and”.
- Marel, Erik van der, “Data Regulation and Digital Services Trade in Africa” (2024) 11:1 Journal of African Trade, online: <<https://jat.afreximbank.com/journal/vol11/iss1/5>>.
- Markovich, Sarit & Yaron Yehezkel, “Data Regulation: Who Should Control Our Data?” (2021) SSRN Journal, online: <<https://www.ssrn.com/abstract=3801314>>.

- Martin, Nicholas et al, “How Data Protection Regulation Affects Startup Innovation” (2019) 21:6 *Inf Syst Front* 1307–1324.
- Matthias Bauer et al, “A methodology to estimate the costs of data regulations” (2016) 146 *International Economics* 12–39.
- Matthias Bauer et al, “The Costs of Data Localisation: Friend fire on economic recovery” (2014) 3 *ECIPE Occasional Paper*.
- Mattoo, Aaditya & Joshua P Meltzer, “International Data Flows and Privacy: The Conflict and its Resolution” (2018) 8431 *World Bank Policy Research Working Paper*, online: <https://papers.ssrn.com/abstract=3175036>.
- Meltzer, Joshua Paul, “The Internet, Cross-Border Data Flows and International Trade” (2015) 2:1 *Asia & the Pacific Policy Studies* 90–102.
- Mira Burri, “Cross-border data flows and privacy in global trade law: has trade trumped data protection?” (2023) 39:1 *Oxford Review of Economic Policy* 85–97.
- Mirzaye, Sina & Muhammad Mohiuddin, “Digital Transformation in International Trade: Opportunities, Challenges, and Policy Implications” (2025) 18:8 *Journal of Risk and Financial Management* 421.
- Mishra, Neha & Kholofelo Kugler, “International Community in the Global Digital Economy: a Case Study on the African Digital Trade Framework” (2024) 73:4 *International & Comparative Law Quarterly* 853–889.
- Mitchell, Andrew D & Neha Mishra, “Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute” (2019) 22:3 *J Int’l Econ L* 389–416.

- Mukiri-Smith, Hellen & Ronald Leenes, “Beyond the ‘Brussels Effect’? Kenya’s Data Protection Act (DPA) 2019 and the European Union’s General Data Protection Regulation (GDPR) 2018” (2021) 7:4 European Data Protection Law Review 502–519.
- Munung, Nchangwi Syntia et al, “Data protection legislation in Africa and pathways for enhancing compliance in big data health research” (2024) 22:1 Health Research Policy and Systems 145.
- Ngqoleka, Sinazo et al, “Industrial Diversification in Emerging Economies: The Role of Human Capital, Technological Investment, and Institutional Quality in Promoting Economic Complexity” (2025) 17:15 Sustainability 7021.
- Nicolaidis, Kalypso & Gregory Shaffer, “Transnational Mutual Recognition Regimes: Governance without Global Government” (2005) 68:3 Law and Contemporary Problems 263–318.
- Nyangweso, Gladys Anne et al, “liberalising cross-border data flows in africa to unlock the continent’s digital economy - an analysis of data flow restrictions in the eac and ecowas economic communities. 07/11/2022”.
- Ogele, Eziho Promise, “The Hegemon’s Role: Nigeria’s Foreign Policy and Its Impact on West African Regional Security and Cooperation.” (2025) 10:1 International Journal Pedagogy of Social Studies 43–56.
- Patrick Leblond, “Trade Agreements and Data Governance” (2024) Centre for International Governance Innovation, online: <<https://www.cigionline.org/articles/trade-agreements-and-data-governance/>>.
- Paul M Schwartz & Karl-Nikolaus Peifer, “Structuring International Data Privacy Law” 21 International Data Privacy Law.

- Quan, Xiaolian, “The Governance of Cross-Border Data Flows in Trade Agreements: Is the CPTPP Framework an Ideal Way out? Focus: Research on the Major Issues of Data Flow and Information Privacy Protection: A Global Watch from a Chinese Perspective” (2020) 15:3 *Frontiers L China* 253–279.
- Rahul Bhatnagar & Julien Gourdon, “E-Commerce: an Essential Lever for Regional Integration in Africa” (2025) 281 *FDI Policy Brief*, online: <<https://ferdi.fr/dl/df-FLRuAJr4G8kJNRUwF6bj4JGT/ferdi-b281-e-commerce-an-essential-lever-for-regional-integration-in-africa.pdf>>.
- Riley, Chris, “Unpacking interoperability in competition” (2020) 5:1 *Journal of Cyber Policy* 94–106.
- Ritter, Jeffrey & Anna Mayer, “Regulating Data as Property: A New Construct for Moving Forward” (2017) 16 *Duke L & Tech Rev* 220.
- Rolf H Weber, “Legal Interoperability as a Tool for Combatting Fragmentation” (2014) *Global Commission on Internet Governance Paper Series* (4) , online: <<https://www.cigionline.org/publications/legal-interoperability-tool-combatting-fragmentation/>>.
- Rotenberg, Julian, “Privacy Before Trade: Assessing the WTO-Consistency of Privacy-Based Cross-Border Data Flow Restrictions” (2021) 28:1 *University of Miami International and Comparative Law Review*.
- Salami, Emmanuel, “Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa” (2022) 66:2 *Journal of African Law* 281–291.

- Schilirò, Daniele, “Digital Transformation, COVID-19, and the Future of Work” (2021) 12:3 IJBMER 1945–1952.
- Schwartz, Paul M, “European Data Protection Law and Restrictions on International Data Flows” (1994) 80 Iowa L Rev 471.
- Schwartz, Paul M, “Information Privacy in the Cloud” 161 University of Pennsylvania Law Review 1623–1662.
- Sedgewick, Margaret Byrne, “Transborder Data Privacy as Trade” (2017) 105:5 California Law Review 1513–1542.
- Selby, John, “Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?” (2017) 25:3 Int J Law Info Tech 213–232.
- Shermon Cruz, “Alternative futures of global governance: scenarios and perspectives from the Global South” (2015) 17:2 The Journal of Futures Studies, Strategic Thinking and Policy 125–142.
- Shumba, W, “Towards the African Economic Community: Legal and Historical Perspectives” (2023) 26:1 Potchefstroom Electronic Law Journal (PELJ) 1–32.
- Simon Züfle, “From silicon valley to silicon savannah: Conceptualizing tech hubs in Sub-Saharan Africa” (2023) The International Journal of Entrepreneurship and Innovation, online: <<https://journals.sagepub.com/doi/epub/10.1177/14657503231221921>>.
- Słok-Wódkowska, Magdalena & Joanna Mazur, “Between commodification and data protection: Regulatory models governing cross-border information transfers in regional trade agreements” (2024) 37:1 Leiden Journal of International Law 111–138.
- Sokol, D Daniel & Roisin Comerford, “Antitrust and Regulating Big Data” (2015) 23 Geo Mason L Rev 1129.

- Solove, Daniel J, “Data Is What Data Does: Regulating Based on Harm and Risk instead of Sensitive Data” (2023) 118 Nw U L Rev 1081.
- Solove, Daniel & Paul Schwartz, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information” (2011) 86 New York University Law Review 1814.
- Soprana, Marta, “The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block” (2021) XIII Trade, Law and Development 143.
- Soulé, Folashadé, “Digital Sovereignty in Africa: Moving beyond Local Data Ownership” (2024) 181 CIGI.
- Staunton, Ciara et al, “Cross-border data sharing for research in Africa: an analysis of the data protection and research ethics requirements in 12 jurisdictions” (2025) 12:1 J Law Biosci Isaf002.
- Sun, Luyao, “Overview of Regulations on Cross Border Data Flow” (2023) 8:1 Academic Journal of Science and Technology 171–176.
- Sun, Ruiqi & Daniel Trefler, “The Impact of AI and Cross-Border Data Regulation on International Trade in Digital Services: A Large Language Model” (2023) NBER Working Paper Series, online: <<https://www.nber.org/papers/w31925>>.
- Suryadevara, Srikanth, “Navigating Data Protection Challenges in the Era of Artificial Intelligence: A Comprehensive Review” (2024) REVISTA DE INTELIGENCIA ARTIFICIAL EN MEDICINA, online: <https://www.academia.edu/124958504/Navigating_Data_Protection_Challenges_in_the_Era_of_Artificial_Intelligence_A_Comprehensive_Review>.

- Susan Ariel Aaronson, “A Difficult Balance Privacy, National Security and the Free Flow of Data” (2025) Center for International Governance Innovation (330) , online: <<https://www.cigionline.org/publications/a-difficult-balance-privacy-national-security-and-the-free-flow-of-data/>>.
- Swales, Lee, “The Protection of Personal Information Act and data de-identification” (2021) 117:7–8 South African Journal of Science 1–3.
- Trachtman, Joel P, “Trade and... Problems, Cost-Benefit Analysis and Subsidiarity” (1998) 9 European Journal of International Law.
- Vásquez Callo-Müller, María & Franziska Sucker, “Evolving approaches to cross-border data flows: Latin American and African perspectives” (2025) 00:00 International Data Privacy Law 1–16.
- Wentong Zheng, “The Digital Challenge to International Trade Law” (2020) 52 International Law and Politics 539–592.
- Wysokińska, Zofia, “A Review of the Impact of the Digital Transformation on the Global and European Economy” (2021) 24:3 Comparative Economic Research Central and Eastern Europe 75–92.
- Xu, Wanxiu, Shuo Wang & Xiaodong Zuo, “Global data governance at a turning point? Rethinking China-U.S. cross-border data flow regulatory models” (2024) 55 Computer Law & Security Review 106061.
- Xu, Wanxiu, Shuo Wang & Xiaodong Zuo, “Whose victory? A perspective on shifts in US-China cross-border data flow rules in the AI era” (2025) 0:0 The Pacific Review 1–27.
- Yakovleva, Svetlana, “Should Fundamental Rights to Privacy and Data Protection be a Part of the EU’s International Trade ‘Deals’?” (2018) 17:3 World Trade Review 477–508.

- Yakovleva, Svetlana & Kristina Irion, “Pitching trade against privacy: reconciling EU governance of personal data flows with external trade” (2020) 10:3 *International Data Privacy Law* 201–221.
- Yang, Min et al, “Laws and Regulations tell how to classify your data: A case study on higher education” (2023) 60:3 *Information Processing & Management* 103240.
- Yeung, Karen, “Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law” (2019) 82:2 *Modern Law Review* 207–239.
- Yik-Chan, Chin & Jingwu Zhao, “Governing Cross-Border Data Flows: International Trade Agreements and Their Limits” (2022) 11:63 *Laws* 1–22.
- Zhao, Zerui, “The Dilemma of Cross-Border Data Flow and the Construction of Mutual Trust Platform in Asia” (2024) 11:4 *Asian Journal of Law and Society* 488–506.
- Zhengge Lv, “The Dilemma of Cross-Border Data Flow Governance in the AIGC Era and the Game of Rules in International Relations” (2025) 213 *SHS Web Conf* 02044.
- “Recommendations to Promote Alignment and Interoperability Across Data Frameworks Related to Cross-border Payments: Consultation report”.

Secondary Materials: Newspaper

- Kumar, Manoj & Manoj Kumar, “India to oppose extended e-commerce tariff ban at WTO meet - sources”, *Reuters* (20 February 2024), online: <https://www.reuters.com/business/retail-consumer/india-oppose-extended-e-commerce-tariff-ban-wto-meet-sources-2024-02-20/>.

Secondary Materials: Reports

- Anne Josephine Flanagan, Nada AlSaeed, & Sheila Warren, *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, by

Anne Josephine Flanagan, Nada AlSaeed, & Sheila Warren (World Economic Forum, 2020).

- Chang, Qing et al, *Production, Trade, and Cross-Border Data Flows*, by Qing Chang et al, www.nber.org, w31416 (National Bureau of Economic Research, 3 July 2023).
- Cory, Nigel, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, by Nigel Cory, ResearchGate (Information Technology and Innovation Foundation, 1 May 2017).
- Cory, Nigel & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them* (2021), online: <<https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>>.
- De Klerk, Kyle, *Energising Africa's Digital Economy: Cross-Border Data Flows and the African Continental FTA*, by Kyle De Klerk, DOI.org (Crossref) (Commonwealth Secretariat, 10 July 2023).
- Deborah James, *Digital Trade Rules: A Disastrous New Constitution For the Global Economy, by and for big tech*, by Deborah James, Zotero (Brussels: Center for Economic and Policy Research, 2020).
- ECA, *Digital trade regulatory environment : opportunities for regulatory harmonization in Africa*, by ECA (Ethiopia: Economic Commission for Africa, 2025).
- Eunice Baguma Ball, Dr Kui Kihoro Mackay, & Stav Bar-Shany, *African Digital Ecosystems Snapshots Ghana, Nigeria, Tanzania & Uganda*, by Eunice Baguma Ball, Dr Kui Kihoro Mackay, & Stav Bar-Shany (AfriconEU Consortium, 2023).

- European Commission, *Annex to the Recommendation for a Council Decision Authorising the Opening of Negotiations for the Inclusion of Provisions on Cross-Border Data Flows in the Agreement Between the European Union and Japan for an Economic Partnership*, by European Commission (Brussels: European Commission, 2022).
- Fefer, Rachel F, *Data Flows, Online Privacy, and Trade Policy*, by Rachel F Fefer, Zotero, R45584 (Congressional Research Service, 2020).
- Ferracane, Martina Francesca & Erik Leendert Van Der Marel, *Regulating Personal Data: Data Models and Digital Services Trade*, by Martina Francesca Ferracane & Erik Leendert Van Der Marel, ocul-qu.primo.exlibrisgroup.com (The World Bank, 2021).
- Fola Adeleke, *Exploring Policy Trade-Offs for data localisation in South Africa, Kenya and Nigeria* (2021) (09).
- GSMA, *The Mobile Economy Africa 2025*, by GSMA, Zotero.
- IFC & Google, *e-Conomy Africa 2020 - Africa's \$180 Billion Internet Economy Future*, by IFC & Google (Washington, D.C, 2020).
- Javier López González & Marie-Agnes Jouanjean, *Digital Trade: Developing a Framework for Analysis*, OECD Trade Policy Papers, by Javier López González & Marie-Agnes Jouanjean, in *OECD Trade Policy Papers*, DOI.org (Crossref), OECD Trade Policy Papers 205 (2017).
- Kholofelo Kugler, *The Impact of Data Localisation Laws on Trade in Africa* (2021) (08), online: <<https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20laws%20and%20trade.pdf>>.

- Leblond, Patrick, *Digital Trade at the WTO: The CPTPP and CUSMA Pose Challenges to Canadian Data Regulation*, by Patrick Leblond, ocul-qu.primo.exlibrisgroup.com (Centre for International Governance Innovation, 2019).
- Lemma, Alberto & Prachi Agarwal, *Implementing the Digital Trade Protocol of the African Continental Free Trade Area*, by Alberto Lemma & Prachi Agarwal, Zotero (London, UK: ODI Global, 2024).
- López González, J & J Ferencz, *Digital Trade and Market Openness*, by López González, J & J Ferencz, in *OECD Trade Policy Papers*, Crossref, No. 217 (Paris: Organisation for Economic Co-Operation and Development (OECD), 2018).
- Martina Francesca Ferracane & Erik Leendert Van Der Marel, *Regulating Personal Data : Data Models and Digital Services Trade*, World Development Report, by Martina Francesca Ferracane & Erik Leendert Van Der Marel, in *Policy Research Working Paper*, World Development Report 9596 (World Bank, 2021).
- Melody Musoni, Poorva Karkare, & Chloe Teevan, *Cross-border data flows in Africa: Continental ambitions and political realities – ECDPM Discussion Paper 379*, by Melody Musoni, Poorva Karkare, & Chloe Teevan (EDPM).
- Morosini, Fábio, Lucas Taschetto & Marília Maciel, *Challenges and Strategies for Latin American Countries in E-commerce and Data Governance Regulation*, by Fábio Morosini, Lucas Taschetto & Marília Maciel, in *Lapeg Paper No 1*, Zotero (2024).
- Prachi Agarwal & Angela Kolongo, *Unlocking Africa's digital trade potential: A guide to implementing the AfCFTA Digital Trade Protocol* (2025).
- Rob Floyd et al, *Macroeconomic Policies Supporting Start-ups in Africa: A Case Study of Kenya*, by Rob Floyd et al (African Center for Economic Transformation (ACET), 2025).

- Sandra Makumbirofa, Jackline Akello, & Nawal Omar, *Cross-border data flows in Africa: An analysis of the alignment with AfCFTA*, by Sandra Makumbirofa, Jackline Akello, & Nawal Omar (Cape Town: Research ICT Africa, 2025).
- Stuart, John, *Implementing the AfCFTA's Digital Trade Protocol*, by John Stuart, JSTOR (South African Institute of International Affairs, 2024).
- Taffere Tesfachew, *Data protection regulations and international data flows: Implications for trade and development*, by Taffere Tesfachew, in *United Nations Publications*, Zotero (Switzerland: United Nations Committee for Trade and Development (UNCTAD), 2016).
- UNCTAD, *Digital Economy Report 2019 Value Creation and Capture: Implications for Developing Countries*, by UNCTAD, Open WorldCat (Geneva: United Nations, 2019).
- World Bank Group, *Regulating Data Protection and Cybersecurity in Africa: Findings from the Global Data Regulation Diagnostic*, by World Bank Group, in *Governance and the Digital Economy in Africa Technical Background Paper Series* (Washington, DC.: World Bank Group, 2023).
- World Bank, *World Development Report 2021: Data For Better Lives*, by World Bank (Washington, D.C: World Bank Group, 2021).
- World Bank Group, *Kenya Digital Economy Assessment Report*, by World Bank Group (Washington, D.C: World Bank, 2019).
- World Bank, *Nigeria: Country Economic Memorandum*, by World Bank Group (Washington, D.C: World Bank, 2021).
- World Bank, *Nigeria Digital Economy Diagnostic Reports*, by World Bank Group (Washington, D.C: World Bank, 2019).

- World Bank, *South Africa Digital Economy Diagnostic Report*, by World Bank Group (Washington, D.C: World Bank, 2019).
- WTO, *Declaration on Global Electronic Commerce*, by WTO, WT/MIN(98)/DEC/2 (World Trade Organization, 3 September 2025).
- WTO, *Global Trade Outlook and Statistics* (2025), online: https://www.wto.org/english/res_e/booksp_e/trade_outlook25_e.pdf.
- Yasmin Ismail, *E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint Statement*, by Yasmin Ismail, Zotero (Geneva: International Institute for Sustainable Development and CUTS International, 2020).
- Yusuf, Badriyya, *Sustainable Data Governance Frameworks in Africa*.

Secondary Materials: Thesis

- Allotey, Asuquo Kofi Essien, *Data Protection and Transborder Data Flows : Implications for Nigeria's Integration into the Global Network Economy* (LL.D., University of South Africa (South Africa), 2014).
- Makulilo, Alex Boniface, *Protection of Personal Data in sub-Saharan Africa* (phd, Bremen University, 2012).
- Mohamed Toure, *Digital Colonialism in Africa* (PhD, University of the Cumberland, 2025).
- Ncheke, Tholoana Rose, *Cross-Border Data Flows in the Digital Economy: An Analysis Between the European Union General Data Protection Regulation and the Southern African Development Community Data Protection Model Law* (LL.M., University of Pretoria (South Africa), 2020).

Secondary Materials: Unpublished Manuscripts

- Ajayi, Muyiwa, “An Analysis of Nigeria’s Legal Framework for Cross-Border Data Transfer: The Afcta Perspective” (17 April 2024) Rochester, NY, online: <<https://papers.ssrn.com/abstract=4798172>>.
- Babalola, Olumide, “The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant” (16 March 2024) Rochester, NY, online: <<https://papers.ssrn.com/abstract=4786872>>.
- Bouke, MA et al, “African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions” (5 July 2023), online: <<http://arxiv.org/abs/2307.01966>>.
- Burri, Mira & Rodrigo Polanco, “Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset” (7 November 2019) Rochester, NY, online: <<https://papers.ssrn.com/abstract=3482470>>.
- Chander, Anupam & Uyen P Le, “Breaking the Web: Data Localization vs. the Global Internet” (2014) Rochester, NY, online: <<https://papers.ssrn.com/abstract=2407858>>.
- Erik van der Marel, “Shifting into Digital Services: Does a Crisis Matter and for Who? |” (16 July 2025), online: <<https://ecipe.org/publications/shifting-into-digital-services/>>.
- Ewulum, Christopher, “The Legal Regime for Cross-border Data Transfer in Africa: a Critical Analysis” (21 August 2023) Rochester, NY, online: <<https://papers.ssrn.com/abstract=4546964>>.
- Gehl Sampath, Padmashree (eds) & Fiona (eds) Tregenna, “Digital Sovereignty: African Perspectives” (15 January 2022), online: <<https://zenodo.org/record/5851685>>.

- Greenleaf, Graham, “Global Data Privacy Laws: 89 Countries, and Accelerating” (6 February 2012) Rochester, NY, online: <<https://papers.ssrn.com/abstract=2000034>>.
- Gyanchandani, Vandana, “Cross-border flow of personal data (digital trade) ought to have data protection” (1 November 2024) Rochester, NY, online: <<https://papers.ssrn.com/abstract=5037955>>.
- Hu, Runshan et al, “Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR” (1 September 2017) Rochester, NY, online: <<https://papers.ssrn.com/abstract=3034261>>.
- Matinou, Samuel Frank et al, “Beyond Borders: Exploring Data Embassies as a Strategy for Digital Sovereignty in Africa” (5 August 2025), online: <<https://preprints.apsanet.org/engage/apsa/article-details/6890b12c23be8e43d6b625fa>>.
- Nevein Elnahrawi, “The Role of Digital Transformation in Africa’s Regional Integration” (2022) Rochester, NY, online: <<https://papers.ssrn.com/abstract=4595317>>.
- Nwosu, Daniel, “Data Localization: The Effects on Cloud Adoption in Nigeria” (5 November 2017) Rochester, NY, online: <<https://papers.ssrn.com/abstract=3065432>>.
- Ojenya, Azeemah, “Cross Border Data Transfer in Digital Trade: Legal Consideration and Best Practices” (5 March 2025) Rochester, NY, online: <<https://papers.ssrn.com/abstract=5185902>>.
- Olayanju Jayeola, Abdulhakeem, “Policy Developments on Cross-Border Data Transfers and Digital Trade in Nigeria” (28 September 2024) Rochester, NY, online: <<https://papers.ssrn.com/abstract=5046169>>.

- Onwudiegwu, Ogonna Annette, “Navigating the Legal Landscape of Cross-Border Data Transfer and Digital Trade in Nigeria” (28 September 2024) Rochester, NY, online: <https://papers.ssrn.com/abstract=5149446>.
- Trudi Hartzenberg, “Regional Integration in Africa” (Staff Working Paper ERSD) Trudi Hartzenberg, World Trade Organization (2011).

Annex A – Coding Manual and Scoring Rules

A.1 Purpose of the Coding Manual

This Appendix details the coding manual and scoring rules for assessing domestic cross-border data flow (CBDF) systems in Nigeria, Kenya, and South Africa. It applies the five-dimensional analytical framework developed in Chapter 2 and used in Chapters 3 and 4. It also provides the method for the diagnostic alignment scorecard found in Section 4.6.

The coding manual serves four purposes. First, it outlines the units of analysis, sources, and coding criteria for consistently examining domestic CBDF systems. Second, it explains the scoring rules used to turn qualitative legal and institutional analysis into structured diagnostic scores. Third, it limits researcher choices by providing clear decision rules, exclusions, and evidence boundaries. Fourth, it allows for a detailed examination of the scorecard by clarifying how scores were created and what they mean.

A.2 Units of Analysis and Sources

The primary focus is the domestic CBDF regulatory system in each case-study area. This system is evaluated as a whole but broken down into the five dimensions set out in chapter 2.7, with each dimension serving as the respective unit of analysis. Each dimension is coded on its own, and the scores given in one dimension do not affect scores in the others. No overall or combined score is created. Coding draws exclusively from authoritative sources, including: Primary legislation (data protection statutes and enabling acts), Subsidiary legislation and binding regulations, Sector-specific statutes and regulatory instruments with CBDF implications, Official regulatory guidance issued by competent authorities. Academic literature and policy reports are used only for interpretive context, not as primary coding inputs.

A.3 AfCFTA CBDF Benchmark Mapping

The AfCFTA CBDF benchmark applied in this thesis is derived from Chapter 3 and reflects a composite of principles rather than a single rule. For coding purposes, benchmark elements are mapped to analytical dimensions as follows:

AfCFTA CBDF Benchmark Element	Relevant Dimension(s)
Conditional permissiveness of CBDF	Dimension 2
Continuity of safeguards across borders	Dimensions 2 and 4
Regulatory interoperability and cooperation	Dimension 3
Legal certainty and transparency	Dimension 1
Protection of data subject rights	Dimension 4
Capacity-sensitive implementation	Dimension 5

This mapping ensures that diagnostic scores are rather than purely domestically comparative.

A.4 Description of Analytical Dimensions, Coding Criteria and Anchor Thresholds

This section operationalizes the five analytical dimensions developed in section 2.7. It does not restate the conceptual justification for the framework. Instead, it specifies how each dimension was coded in practice for the purposes of the diagnostic assessment in Chapter 4 and the alignment scorecard in Section 4.6. Scores are ordinal and dimension-specific and must not be aggregated.

Dimension 1: Legal–Normative Foundations

- Coding question: How is cross-border data flow (CBDF) legality constituted within the domestic legal system?
- Indicators are: Location of CBDF rules (primary legislation vs subsidiary instruments); Degree of normative consolidation or fragmentation; Hierarchy and interaction of

applicable legal norms; Exclusions; Enforcement outcomes; Institutional capacity; Sector-specific effects

Anchor thresholds

5 – CBDF rules consolidated in primary legislation with high internal coherence

4 – Primary legislation with limited reliance on delegated instruments

3 – Primary legislation supplemented by significant delegated or sector-specific rules

2 – Fragmented legal basis with weak normative hierarchy

1 – No coherent legal basis for CBDF

Dimension 2: Substantive Regulatory Scope

- Coding question: Under what substantive conditions are cross-border data transfers permitted, restricted, or conditioned?
- Indicators are: Transfer gateways (e.g. adequacy, consent, contracts, public interest); Onward-transfer controls; Sector-specific localization or approval requirements
- Exclusions are: Institutional enforcement capacity; Rights enforcement outcomes

Anchor thresholds

5 – Clear transfer gateways with minimal sectoral derogations

4 – Gateways exist with limited sector-specific constraints

3 – Gateways exist, but administrative discretion materially shapes legality

2 – Multiple sector-specific constraints significantly narrow CBDF operability

1 – CBDF effectively prohibited or blocked

Dimension 3: Institutional and Implementation Mechanisms

- Coding question: How are CBDF rules administered, enforced, and coordinated institutionally?

- Indicators are: Existence and statutory footing of a supervisory authority; Enforcement tools (complaints, investigations, orders, sanctions); Coordination mechanisms and legal status of regulatory instruments;
- Exclusions are: Enforcement effectiveness in practice; Market uptake or compliance rates;

Anchor thresholds

- 5 – Integrated authority with clear coordination and enforcement powers
- 4 – Strong authority with minor coordination limitations
- 3 – Authority exists but relies heavily on administrative discretion
- 2 – Fragmented institutional environment with overlapping mandates
- 1 – No effective supervisory framework

Dimension 4: Rights and Digital Safeguards

- Coding question: What rights and safeguards apply to data subjects in cross-border processing contexts?
- Indicators are: Data subject rights affecting international transfers; Security safeguards and breach-notification obligations; Accountability mechanisms for foreign processing
- Exclusions are: Empirical enforcement rates; Institutional capacity constraints

Anchor thresholds

- 5 – Comprehensive rights with strong accountability and remedies
- 4 – Robust rights with moderate remedial intensity
- 3 – Core rights present but operational clarity limited
- 2 – Rights uneven or heavily qualified
- 1 – Minimal or absent safeguards

Dimension 5: Socio-Economic and Technical Context

- Coding question: Do domestic legal design features structurally support or constrain the operability of CBDF governance?
- Indicators are: Allocation of compliance and assessment burdens under domestic law; Degree of regulatory layering and complexity; Reliance on decentralized compliance assessment mechanisms
- Exclusions are: Development level; Infrastructure quality; Enforcement success or failure

Anchor thresholds

- 5 – Legal design strongly reinforces CBDF operability
- 4 – Legal design broadly supports operability with limited rigidity
- 3 – Legal design neither clearly enables nor disables operability
- 2 – Legal design significantly complicates CBDF operability
- 1 – Legal design renders CBDF implementation impracticable

The numerical symmetry of the anchor scale does not imply substantive equivalence across dimensions. Each dimension captures a distinct analytical concern identified in Chapters 1–4.

Scores are diagnostic and comparative, not evaluative or predictive.

A.5 Scoring Rules and Constraints

1. Comparative Rule: Scores are relative, not absolute.
2. No-Outcome Rule: Scores do not reflect enforcement outcomes.
3. No-Compensation Rule: Strength in one dimension does not offset weakness in another.
4. Conservative Assignment Rule: Ambiguity resolves downward.
5. Dimension-5 Constraint Rule: Scores reflect operability risk only.

A.6 Scoring Workflow

Scores are assigned through the following workflow:

1. Identify all domestic instruments relevant to CBDF (primary, delegated, sectoral).
2. Extract CBDF-relevant provisions with pinpoint citations into a coding log.
3. Assign extracted provisions to relevant dimension indicators.
4. Apply dimension-specific anchor thresholds to generate a preliminary score.
5. Apply the conservative assignment rule (described in A.5 above) where evidence is ambiguous.
6. Check for compliance with the no-compensation rule (described in A.5 above) across dimensions.
7. Record final scores in a coding log with brief justification sentences cross-referenced to Chapter 4 (see author’s coding log in A.7 below).

A.7 Coding Log with Evidence

Nigeria

Row	Country	Dimension	Pinpoint authority	Coding signal (what it evidences)	Score (relevance)
NG-01	Nigeria	D1	NDPA 2023, s 1(1)(a)–(h) (objectives)	Rights governance framing; “trusted use” and participation in regional/global economies +	Strong statutory normative base (rights + trade-facing objectives)

				explicitly included	
NG-02	Nigeria	D1	NDPA 2023, s 24 (principles) (Arrangement + Part V heading)	Modern data protection principles as baseline architecture	Supports “comprehensive statute” score in D1
NG-03	Nigeria	D1	NDPA 2023, s 25 (lawful bases) (Arrangement)	Processing legitimacy is statute-defined (not purely consent-driven)	Increases legal robustness / interoperability potential
NG-04	Nigeria	D2	NDPA 2023, s 41(1)(a)–(b) (cross-border transfer gateway)	Default rule: transfers only with “adequate protection” instruments or s 43 bases	Core CBDF restrictiveness/conditionality metric
NG-05	Nigeria	D2	NDPA 2023, s 41(2) (record basis)	Accountability: must document transfer basis	Improves governance quality but increases

					compliance friction
NG-06	Nigeria	D2	NDPA 2023, s 41(4) (extra restrictions categories)	Commission can tighten transfers by categories of data	Strong sovereignty lever → may reduce AfCFTA “openness” alignment
NG-07	Nigeria	D2	NDPA 2023, s 42(2)(a)–(f) (adequacy criteria)	Structured adequacy test (rule of law, DPA, redress, commitments etc.)	Raises “trust” but may slow intra-Africa flows absent determinations
NG-08	Nigeria	D2	GAID 2025, cross-border transfer review criteria (builds s 42 factors; mutual assistance emphasis)	Makes adequacy logic operational; expects cooperation instruments	Supports D2 maturity (“law-in-action” guidance)

NG-09	Nigeria	D2	GAID 2025, “Cross-Border Data Transfer” assessment table (explicitly references ss 41–42)	Practical compliance steps: countries, safeguards, justification	Demonstrates implementability (not just aspirational drafting)
NG-10	Nigeria	D3	NDPA 2023, ss 4–7 (Commission + independence) (Arrangement lines)	Dedicated regulator with statutory “independence” hook	Institutional credibility metric
NG-11	Nigeria	D3	NDPA 2023, ss 5–6 (functions + powers) (Arrangement lines)	NDPC can regulate, guide, and supervise	Capacity to run CBDF regime, including approvals/guidelines
NG-12	Nigeria	D3	NDPA 2023, Part X (complaints/investigations; compliance/enforcement orders; penalties)	Full enforcement pipeline exists (administrative + penalties)	Raises enforceability score if used in practice

NG-13	Nigeria	D3	NDPA 2023, s 44 (registration “of major importance”) (Arrangement)	Regulatory perimeter tool for high-impact entities	Practical implementation lever for CBDF monitoring
NG-14	Nigeria	D4	NDPA 2023, s 34(1)(a)(iii) (right to know foreign recipients)	Data subject visibility of third-country transfers	Strong rights-based CBDF safeguard
NG-15	Nigeria	D4	NDPA 2023, s 34(1)(c)–(e) (correction/erasure/restriction)	Remedial rights affecting onward/continued processing	Strong “trust” signal and cross-border risk mitigation
NG-16	Nigeria	D4	NDPA 2023, ss 35–36 (withdraw consent; object)	Rights that can constrain transfer-based processing	Raises D4 strength; may increase operational friction
NG-17	Nigeria	D5	GAID 2025, “data sovereignty considerations” in CB transfer	State capacity + sovereignty	Evidence of technical/po

			assessment (public service/government function; access; remedies)	framing baked into compliance practice	licy constraints shaping CBDF in practice
NG-18	Nigeria	D5	NDPA 2023, s 63 (priority of Act) (Arrangement)	Priority rule exists (conflict-resolution tool)	Helps manage overlap with sectoral rules (but does not erase them)
NG-19	Nigeria	D5	NDPA 2023, s 3(2)(a)–(e) (exemptions: security, criminal justice, public health, etc.)	Operational carve-outs that matter for government/critical sectors	Real-world limits on “uniform” CBDF governance

Kenya

Row	Country	Dim	Pinpoint authority	Coding signal (what it evidences)	Score (relevance)
-----	---------	-----	--------------------	-----------------------------------	-------------------

KE-01	Kenya	D1	KDPA 2019, long title + general structure (statute-based model)	Rights + governance rationale anchored in a comprehensive Act	Strong legal foundations (not guidance-only)
KE-02	Kenya	D1	KDPA 2019, Part VI (transfers) exists as statutory architecture	CBDF is not incidental; it is explicitly legislated	Supports D1 + D2 readiness
KE-03	Kenya	D1	KDPA 2019, establishment of ODPC / Commissioner (statutory regulator) (as referenced in chapter draft)	Institutional embedding is statute-led	Supports baseline institutional legitimacy
KE-04	Kenya	D2	KDPA 2019, s 48 (default safeguard test for transfers outside Kenya)	Conditional transfer model (proof of safeguards to Commissioner)	Core CBDF openness/restrictiveness metric
KE-05	Kenya	D2	Data Protection (General) Regulations 2021 (cross-border transfer provisions)	Implementing detail for transfer safeguards and	Boosts maturity (“how

				operational requirements	transfers happen”)
KE-06	Kenya	D2	KDPA 2019 (ODPC power to assess/approve safeguards for transfers) (statutory hook in Part VI context)	Regulator-gated interoperability model	Affects speed and predictability of CBDF
KE-07	Kenya	D2	Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021	Compliance perimeter: who must register and how ODPC monitors	Improves monitoring; increases compliance cost
KE-08	Kenya	D2	ICT Authority / national cloud standards/policy (where applicable)	Technical policy constraints can nudge hosting choices	D5 spillover into transfer/localisation “in practice”
KE-09	Kenya	D3	KDPA 2019: ODPC oversight/enforcement model (statutory)	Centralised enforcement architecture	Institutional coherence vs fragmented sector regulators

KE-10	Kenya	D3	Data Protection (Complaints Handling and Enforcement Procedures) Regulations (subsidiary enforcement rules)	Makes enforcement procedurally usable (complaints, investigations)	Strong “law-in-action” indicator
KE-11	Kenya	D3	KDPA 2019 (administrative enforcement powers)	ODPC can act (not just advisory)	Raises enforceability score if resourced
KE-12	Kenya	D3	Data Protection (General) Regulations 2021 (DPIA/recordkeeping operationalisation)	Builds compliance tooling for risk management	Adds implementability to D3
KE-13	Kenya	D4	KDPA 2019 (data subject rights architecture)	Rights baseline that constrains risky transfers	D4 strength driver
KE-14	Kenya	D4	KDPA 2019 (consent + lawful processing framework)	Processing legitimacy and consent quality affect transfers	Rights and safeguards depth (not mere formality)

KE-15	Kenya	D4	KDPA 2019 (security obligations + breach response framework)	Security baseline necessary for “free flow with trust”	D4 score driver
KE-16	Kenya	D5	ODPC institutional maturity + implementing regulations density (General + Registration + Enforcement regulations) (“Thick” secondary framework suggests implementability, but also administrative burden	D5 indicator (practical operability)
KE-17	Kenya	D5	Kenya health sector digital health statute/strategy (where it imposes governance/hosting expectations)	Sectoral digitisation pressure affects CBDF (health data sensitivity)	Contextual constraint (not a transfer rule by itself unless explicit)
KE-18	Kenya	D5	Kenya financial sector outsourcing / ICT risk	Outsourcing/cloud risk controls can	Contextual “soft

			guidance (CBK/financial regulators)	indirectly constrain cross-border processing	localisation” pressure
KE-19	Kenya	D5	Kenya communications/cybersecurity guidance for telecom/ICT sector	Cyber posture influences whether cross-border cloud is acceptable	D5 “technical readiness” proxy

South Africa

Row	Country	Dim	Pinpoint authority	Coding signal (what it evidences)	Score relevance
SA-01	South Africa	D1	POPIA 2013 (purpose + conditions architecture)	Comprehensive rights-based statute (early mover)	Strong normative baseline
SA-02	South Africa	D1	POPIA Regulator/Information Regulator role (statutory scheme)	Institutional legitimacy built into the privacy system	Supports D1/D3
SA-03	South Africa	D1	POPIA “conditions for lawful processing” design (core structure)	Predictable rule-set (not ad hoc guidance)	Interoperability-friendly

SA-04	South Africa	D2	POPIA, s 72 (transborder information flows)	Cross-border transfers allowed only under specified conditions	Core CBDF gateway test
SA-05	South Africa	D2	POPIA, s 72(1)(a)–(c) (typical conditions: adequate protection/consent/contract etc., per statute text)	Mix of adequacy-like protection + derogations model	Determines openness vs “trust” posture
SA-06	South Africa	D2	Information Regulator guidance note (interpretation/expectations re s 72 of POPIA)	Practical interpretation reduces uncertainty for businesses	Improves operability of CBDF regime
SA-07	South Africa	D3	POPIA enforcement architecture (Regulator powers + compliance/enforcement) (System has tools to compel compliance	D3 credibility depends on capacity
SA-08	South Africa	D3	POPIA Regulations (procedural rules)	Secondary instruments for operational enforcement	“Law-in-action” enablement

SA-09	South Africa	D3	POPIA (information officer/accountability governance model)	Internal compliance governance expected within controllers	Raises implementation readiness
SA-10	South Africa	D4	POPIA “security safeguards” (core condition)	Baseline security obligation to support trusted transfers	Key D4 safeguard
SA-11	South Africa	D4	POPIA breach/incident response expectations (statutory + Regulator guidance)	Breach notification and accountability expectations	Trust infrastructure for CBDF
SA-12	South Africa	D4	POPIA data subject rights (access/correction/objection etc.)	Rights enforceability affects transfer legitimacy and onward processing	D4 strength driver
SA-13	South Africa	D5	Cybercrimes Act 2020 (relevant to reporting/cooperation on cyber incidents)	Broader cyber posture supporting trust environment	Contextual readiness for CBDF
SA-14	South Africa	D5	National Cybersecurity Policy Framework	National security + infrastructure posture influences hosting choices	Contextual “security-driven constraints”

SA-15	South Africa	D5	POPIA’s maturity timeline (in-force status + implementation practice)	Older regime → more settled compliance market	D5: ecosystem maturity indicator
-------	--------------	----	---	---	----------------------------------

A.8 Evidence–Anchor Mapping (Anchor-Scale Traceability Table)

This table maps the evidence rows in A.7 above to the dimension-specific anchor thresholds in A.5, demonstrating how final diagnostic scores were assigned in section 4.6.

Dimension 1 – Legal–Normative Foundations

Country	Evidence rows	Score/ Anchor triggered	Mapping explanation
Nigeria	NG-01, NG-02, NG-03	Anchor 3	NDPA provides a comprehensive statutory base (NG-01–03), but CBDF governance is materially supplemented by GAID and sectoral overlays
Kenya	KE-01, KE-02, KE-03	Anchor 4	KDPA is statute-centric and internally coherent; subsidiary regulations operationalize rather than displace the Act
South Africa	SA-01, SA-02, SA-03	Anchor 5	POPIA embeds CBDF legality, principles, and accountability directly in primary legislation, while subsidiary regulations and codes of conduct operate in a strictly subordinate and harmonized manner without creating sector-specific CBDF transfer regimes.

Dimension 2 – Substantive Regulatory Scope

Country	Evidence rows	Score/ Anchor triggered	Mapping explanation
Nigeria	NG-04– NG-09	Anchor 2	NDPA ss 41–42 establish conditional gateways, but Commission-controlled tightening powers and sectoral overlays materially narrow effective CBDF space
Kenya	KE-04– KE-07	Anchor 3	Statutory transfer gateways exist, but regulator-mediated safeguards and approvals introduce discretion that shapes legality in practice
South Africa	SA-04– SA-06	Anchor 4	POPIA s 72 provides clear gateways with limited sectoral derogation and predictable interpretation

Dimension 3 – Institutional & Implementation Mechanisms

Country	Evidence rows	Score Anchor triggered	Mapping explanation
Nigeria	NG-10– NG-13	Anchor 2	NDPC exists with statutory powers, but registration thresholds, sectoral regulators, and executive instruments create fragmentation
Kenya	KE-09– KE-12	Anchor 3	ODPC is central and statute-based, but enforcement and approvals are discretion-heavy and capacity-dependent

South Africa	SA-07– SA-09	Anchor 4	Information Regulator has clear statutory powers and procedures, with fewer coordination frictions
--------------	-----------------	----------	--

Dimension 4 – Rights and Digital Safeguards

Country	Evidence rows	Score Anchor triggered	Mapping explanation
Nigeria	NG-14– NG-16	Anchor 3	NDPA provides core rights and safeguards, but enforcement maturity and interaction with sectoral regimes limit operational clarity
Kenya	KE-13– KE-15	Anchor 4	KDPA establishes strong rights and safeguards, with clearer administrative pathways
South Africa	SA-10– SA-12	Anchor 5	POPIA combines extensive rights, accountability, and remedies with mature breach/security obligations

Dimension 5 – Socio-Economic & Technical Context (Operability Risk)

Country	Evidence rows	Score/Anchor triggered	Mapping explanation
Nigeria	NG-17– NG-19	Anchor 2	Sovereignty-heavy assessment criteria, broad exemptions, and layered oversight significantly increase compliance friction

Kenya	KE-16– KE-19	Anchor 3	Dense subsidiary framework enables compliance but imposes administrative load without categorical obstruction
South Africa	SA-13– SA-15	Anchor 4	Mature ecosystem, settled guidance, and cyber governance reinforce operability despite higher compliance standards

A.9 Use, Limits, and Replicability

The scorecard is a diagnostic instrument designed to identify sources of alignment and misalignment relevant to the implementation of AfCFTA CBDF. It is not a ranking, index, or compliance assessment. Another researcher applying this coding manual to the same legal sources should be able to reproduce the reasoning process, identify points of interpretive discretion, and generate broadly comparable alignment profiles, even if individual scores differ at the margins.