CROSS-BORDER DATA FLOWS IN AFRICA: EXPLORING LEGAL FRAMEWORKS AND REGIONAL IMPORTANCE

Strathmore University

Centre for Intellectual Property and Information Technology Law

TABLE OF CONTENTS

ACKNOWLEDGEMENT

The preparation and publication of this report have been made possible through funding from the **Hewlett Foundation**. We would like to thank the organisation for their continued support. CIPIT wishes to extend gratitude to the team whose collaboration made this report possible. We particularly appreciate the efforts of the authors, Research Assistant **Calvin Mulindwa** and Research Intern **Gia Sajan**, for their research and drafting, which shaped the content of the report. We are equally grateful to **Joshua Kitili**, whose editorial insight significantly enhanced both the quality and scope of the final publication. Lastly, we wish to thank the **administrative team** for their continued support throughout the process of developing this report, as well as **Jacala Solutions Ltd** for designing the final version.

EXECUTIVE SUMMARY

This report presents a comprehensive analysis of cross-border data flows in Africa, focusing on the interaction between free trade agreements, domestic legal frameworks, and data protection principles. The study examines the significant role that cross-border data flows play in the global economy, particularly in the digital age, where data is a critical asset for economic growth, innovation, and international trade.

The report identifies key challenges facing African nations in harmonising their data protection laws, which are crucial for facilitating cross-border data flows. These challenges include discrepancies in regulatory frameworks, the need for robust data protection mechanisms, and the impact of data localisation policies on economic growth. Additionally, the report highlights the importance of adopting international standards to ensure that data protection frameworks across Africa are compatible with global practices, thereby enhancing the continent's participation in the global digital economy.

Moreover, the analysis underscores the role of free trade agreements (FTAs) in promoting data flows by reducing regulatory barriers and fostering a more integrated digital market. Specific case studies from African countries illustrate how FTAs can influence domestic data policies, either by encouraging the adoption of more liberal data flow regulations or by imposing stricter data protection requirements in line with international standards.

The report concludes with several recommendations for policymakers and businesses in Africa. Policymakers are urged to harmonise data protection laws across the continent, improve digital infrastructure, and engage in regional cooperation to create a conducive environment for cross-border data flows. Businesses are advised to invest in data protection compliance and leverage technological innovations to enhance their competitiveness in the global market.

By addressing these challenges and implementing the proposed recommendations, Africa can better harness the potential of cross-border data flows to drive economic growth, innovation, and regional integration. The report ultimately calls for a coordinated effort among African governments, businesses, and regional bodies to build a resilient and secure digital economy that benefits all stakeholders.

1.0 Introduction

Data refers to facts, figures, or information that can be used to make decisions, perform analyses, or operate systems. In the context of cross-border data flows, data can include a wide range of types, such as personal data (like names, addresses, and payment information), corporate data (such as business records, intellectual property, and proprietary information), government data (policy documents and statistical information), and transactional data (details of online transactions).[1] This data is transmitted across borders primarily through digital networks, where it is broken down into packets and routed through different countries before reaching its destination.[2] The transmission methods include using the internet, cloud storage services, and other digital communication channels that facilitate the smooth and secure transfer of data between nations.

Data transfers have grown in value over the recent past based on the utility of data.[3] Its economic value and complexities surrounding classification has often resulted in the need for regulatory frameworks both nationally and internationally.[4] Unlike physical goods, data flows across borders effortlessly, often bypassing traditional trade barriers.[5] This difference has introduced significant complexities in developing legal frameworks for the free flow of data. Traditional trade policies were designed to regulate the movement of tangible goods, whereas data flows require new considerations around privacy, security, and sovereignty.[6] These complexities have necessitated the creation of specialised regulations that address the unique challenges of cross-border data transfers, balancing the need for free data flow with the protection of individual rights and national interests.[7] Its ability to be used by many without running out, along with the low cost of reusing it, are key factors in its economic impact.[8] Processes conducted by firms in sourcing, processing, storing and protecting data has resulted in a sense of dependency in the economy.[9]

When data transfers occur between national boundaries, resulting in the digital flow of the said data or information, it is termed as 'cross-border data flow'.[10] A variety of approaches have been identified to categorise the ways in which cross-border data flows occur. At one end of the spectrum, there may be no regulatory mechanisms in place at all, allowing for a "free flow" of data. Moving along the spectrum, data flows might be allowed but only if specific safeguards are in place, such as compliance with privacy or security standards.

1 Francesca Casalini and Javier López González, 'Trade and Cross-Border Data Flows' (2019) OECD Trade Policy Papers, No. 220 <http://dx.doi.org/10.1787/b2023a47-en> accessed 6 July 2024.
2 Ibid.
3 Cross Border Data Alliance <https://globaldataalliance.org/wp-content/uploads/2021/07/gdafactsandfigures.pdf > accessed on 26 August 2024.
4 Francesca Casalini and Javier López González (n 1).
5 Andrew D Mitchell and Neha Mishra 'WTO Law and Cross Border Data Flows - An Unfinished Agenda, Cambridge University Press <WTO Law and Cross-Border Data Flows (Chapter 4) - Big Data and Global Trade Law (cambridge.org)> accessed 26 August 2024.
6 Ibid.
7 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) WTR <https://doi.org/10.1017/S1474745615000014> accessed 6 July 2024.
8 Franziska Sucker and Alexander Beyleveld, 'Cross-border data flows in Africa: Policy considerations for the AFCFTA Digital Trade protocol' (2022) Report, Mandela Institute <https://ssrn.com/abstract=4278748> accessed 6 July 2024.
9 Susan Aaronson, 'Data is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows' (2018) CIGI Papers No. 197 < https://ssrn.com/abstract=3589861> accessed 6 July 2024.
10 UNCDF, 'The Role of Cross-Border Data Flows in the Digital Economy' (2022) Brief, <https://policyaccelerator.uncdf.org/all/brief-cross-border-data-flows> accessed 6 July 2024.

At the most restrictive end, data flows may be subject to ad-hoc authorisations or other stringent requirements before being permitted. The extent to which these restrictions apply is closely tied to the regulatory frameworks established in each country. The varying degrees of control reflect different national priorities and concerns, ranging from economic interests to privacy and national security.[11] Data in this context can be linked to personal data or a product of digital trade purely.[12]

The scope of this report encompasses an in-depth examination of cross-border data flows in the context of Africa's digital economy. It covers various dimensions including the legal, economic, and technological factors that affect data transfers between countries. The report also delves into specific case studies of African nations to compare and contrast different domestic data protection laws and their impact on cross-border data transfers. Additionally, it evaluates the role of regional and international free trade agreements in facilitating or hindering data flows, with a particular focus on the alignment of these agreements with global data protection standards.

11 Casalini and González (n1).
12 Nelly Rotich, 'Examining Cross-Border Data Flows Provisions in Africa's Free Trade Agreements' (CIPIT , 31 August 2023) <https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/> accessed 6 July 2024.

2.0 Research Objectives

The objectives of the study were as follows:

1. To examine the current landscape of cross-border data flows in Africa and assess how these flows are regulated under domestic legal frameworks and free trade agreements.
2. To provide an understanding of the legal, economic and technological factors that shape data transfers within Africa.
3. To evaluate the potential benefits and challenges that arise from the transfer of data across national boundaries, including concerns related to privacy, security, and data sovereignty.
4. To offer recommendations to policymakers and businesses on how to navigate the regulatory environment surrounding cross-border data flows.

3.0 Methodology

The study employed a desktop research approach, utilising qualitative and quantitative analysis to examine the factors influencing cross-border data flows in Africa. The research involved an extensive review of existing literature, legal documents, policy papers, and case studies. The report also analysed trade agreements, focusing on their specific provisions on data flows, through the examination of both primary and secondary sources available online and in digital archives.

4.0 Tracing Policy Implications and Economic Transformation of Cross Border Data Flows

On 27 June 2014 The African Union adopted the Convention on Cyber Security and Personal Data Protection also known as the Malabo convention.[13] The convention aims to enhance the security of electronic transactions, communications and the protection of critical infrastructure;[14] by establishing clear rules on cybersecurity and data protection, the convention aims to build trust in digital services, boost e-commerce, and enhance the overall digital economy in Africa.[15] It seeks to safeguard the privacy and personal data of individuals by setting standards for the collection, processing and storage of data and establishes guidelines for data protection authorities in African countries to ensure compliance with these standards.[16] The Malabo Convention entered into force in 2023.[17]

On 31 January 2015, The African Union adopted Agenda 2063; it is a document that details that aspirations and goals Africa seeks to achieve.[18] One of its key visions is the establishment of the necessary infrastructure to support Africa's accelerated integration, growth, and technological transformation. This includes the development of high-speed railway networks, roads, shipping lines, sea and air transport, alongside advanced ICT systems and a robust digital economy.[19] The plan envisions a Pan-African High-Speed Train Network connecting major cities and capitals, with accompanying highways, pipelines for gas, oil, water, and broadband cables.[20] This infrastructure is expected to drive manufacturing, skills development, technological innovation, research, integration, and intra-African trade, while also boosting investments and tourism. In relation to cross-border data flows, Africa envisions having the digital infrastructure in place to fully support the continent's economic growth and integration.

On 21 March 2018, the African Union adopted the African Continental Free Trade Area (AfCFTA) and officially came into force on 30 May 2019. The AfCFTA officially commenced

13 AU, 'African Union on Cyber Security and Personal Data Protection' <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed 16 September 2024.
14 AU, Chapter III 'African Union on Cyber Security and Personal Data Protection' <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed 16 September 2024.
15 AU, Section III 'African Union on Cyber Security and Personal Data Protection' <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed 16 September 2024.
16 AU, Chapter II AU, 'African Union on Cyber Security and Personal Data Protection' <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed 16 September 2024.
17 The convention required 15 ratifications to come into force, Mauritania was the latest country to ratify < <2305121.pdf (dataprotection.africa)> accessed 16 September 2024.
18 AU, 'Agenda 2063: The Africa We Want' <Agenda 2063: The Africa We Want. | African Union (au.int)> accessed 16 September 2024.
19 AU 'Agenda 2063: 'The Africa We Want' para 25 <36204-doc-agenda2063_popular_version_en.pdf (au.int)> accessed 16 September 2024.
20 Ibid.

on 1 January 2021. It aims to create a single continental market for goods and services, facilitate the movement of capital and people; and deepen regional integration across Africa.

The AfCFTA seeks to increase trade between African countries by reducing tariffs and other barriers thus promoting the free flow of goods and services across borders.[21] The agreement also aims to enhance industrialisation, economic diversification and sustainable development by enabling African countries to collaborate effectively and expand their markets.[22]

In the context of cross-border data flows, AfCFTA recognises the importance of digital trade and the digital economy in supporting its broader goals.[23] The free movement of data across borders is crucial for modern trade, particularly for sectors like e-commerce, financial services, telecommunications, and technology. Efficient cross-border data transfers allow businesses to operate smoothly across national borders, enhance trade logistics, and drive innovation.

In February 2022, The African Union adopted the AU Data Policy Framework.[24]It aims to create a harmonised and coordinated approach that facilitates the free and secure movement of data across borders while addressing the varying levels of development and regulatory capacity across African countries.[25]

The Framework emphasises the need for African nations to strike a balance between enabling cross-border data flows that support digital trade and economic growth, and implementing safeguards that protect personal data and privacy.[26] It recognises the different data governance regimes — open transfers, conditional transfers, and limited transfer models — and encourages countries to adopt the model that best aligns with their national security, public policy, and development priorities. This allows countries to regulate cross-border data flows in a manner that suits their specific economic and regulatory contexts.[27]Given Africa's varying levels of digital infrastructure, the framework also highlights the need to address these deficiencies, such as through the use of cloud services and the creation of data centres, to support the safe and efficient transfer of data across borders.[28]

Ultimately, Africa is actively working towards creating a single continental market that encourages the free and secure flow of data across borders, while recognising and safeguarding the rights of data subjects. Through initiatives such as the Malabo Convention the continent has laid the foundation for enhancing cybersecurity and personal data protection, it provides a robust framework for securing electronic transactions, communications, and critical infrastructure, with the aim of building trust in digital services, boosting e-commerce, and supporting the digital economy.

21 AU, 'Agreement Establishing the African Continental Free Trade Areas' <36437-treaty-consolidated_text_on_cfta_-_en.pdf (au.int)> accessed 16 September 2024.
22 Ibid.
23 African Union <Home - AfCFTA (au-afcfta.org)> accessed 16 September 2024.
24 AU, 'African Union Data Policy Framework' <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed 16 September 2024.
25 Ibid.
26 AU, 'Africa Union Data Policy Framework', 41 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed 16 September 2024.
27 AU, 'African Union Data Policy Framework', 43 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed 16 September 2024.
28 Ibid.

Furthermore, Agenda 2063, outlines Africa's vision for technological transformation, including the development of infrastructure necessary to support cross-border data flows and broader economic integration. The launch of the AfCFTA also reinforces this goal by promoting regional integration and trade through the free movement of goods, services, and capital. In this context, cross-border data transfers play a crucial role in modernising trade, particularly for key sectors such as e-commerce, finance, and technology.

5.0 Key technologies enabling cross-border data flows

The movement of data across borders has become critical for the functioning of the global economy, particularly in sectors such as e-commerce, finance, telecommunications, and healthcare. As businesses and governments increasingly rely on the transfer of data to operate efficiently, various technologies have emerged to facilitate the secure and seamless flow of information between countries. These technologies play a crucial role in enabling digital trade, driving innovation, and supporting global connectivity. Below are some of the key technologies that are enabling cross-border data flows.

Cloud computing is one of the most important technologies enabling cross-border data flows. It allows users to store, process, and manage data on remote servers rather than local systems.[29] This technology facilitates the rapid movement of data across borders by

29 Microsoft, 'What is Cloud computing?' <What Is Cloud Computing? | Microsoft Azure> accessed 16 September 2024

offering scalable and flexible infrastructure that businesses can access from anywhere in the world.

Internet of Things (IoT) refers to a network of interconnected devices that collect, share, and transmit data over the internet.[30] IoT technology enables real-time data collection and analysis across borders, making it essential for industries such as manufacturing, logistics, and healthcare. IoT devices collect data from different locations, and this information can be transferred across borders to centralised systems for processing and decision-making.[31] For example, sensors in a factory in one country can send data to a server in another country for analysis, enabling more efficient operations and resource management.

Notably, the advent of 5G technology is revolutionising the speed and efficiency of cross-border data flows. 5G networks provide faster data transfer rates, reduced latency, and improved connectivity, allowing businesses to transmit large amounts of data across borders in real-time.[32] This is especially important for industries such as autonomous vehicles, healthcare, and virtual reality, which rely on the fast transmission of data to function effectively.[33] The deployment of 5G networks is expected to enhance the capabilities of cloud computing, IoT, and other technologies, further enabling seamless cross-border data flows.

Equally important are data centres, which play a central role in storing and managing data that flows across borders.[34] These facilities house vast amounts of data and are strategically located to ensure that data can be accessed quickly and securely from different parts of the world.[35] As data volumes increase, the need for data centres near border regions is growing to reduce latency and improve data transfer speeds.

Finally, data encryption is essential for ensuring the security and privacy of data as it moves across borders.[36] Encryption technologies protect data by converting it into an unreadable format that can only be deciphered by authorised users with the correct decryption key.[37] This ensures that even if data is intercepted during transmission, it cannot be accessed by unauthorised parties.[38] Secure data encryption is particularly important for industries such as finance, healthcare, and government, where sensitive information must be protected.

6.0 Economic benefits of enhanced Cross-border data flows

Cross-border data flows have significantly contributed to economic benefits by enabling global businesses to operate more efficiently, increasing innovation, and fostering economic growth. One of the key ways cross-border data flows drive economic growth is by enabling

30 IBM, 'What is the IoT?' <What is the Internet of Things (IoT)? | IBM> accessed 16 September 2024.
31 Ibid.
32 Global Data Alliance, 'Cross Border Data Transfers & Telecommunications and Network Technologies' <Cross-Border Data Transfers & Telecommunication and Network Technologies (globaldataalliance.org)> accessed 16 September 2024.
33 Lalit Chetteri and Rabindranath Bera, 'A Comprehensive Survey on Internet of Things (IoT) Towards 5G Wireless Systems' (2020) 7 (1) IEEE Internet of Things Journal.
34 IBM. 'What is a data centre?' <What Is a Data Centre? | IBM> accessed 16 September 2024.
35 Ibid.
36 Intersect Consulting, 'GDPR Encryption' <Encryption - General Data Protection Regulation (GDPR) (gdpr-info.eu)> accessed 16 September 2024
37 Fatima Abdillahi Farah, Privacy Enhancing Technologies: An Analysis of Implementing Encryption and Pseudonymization to Ensure Personal Data Protection During Third-Country Transfers (Master Thesis, Faculty of Law, Spring Semester 2024).
38 Ibid.

businesses to access global markets and expand their reach beyond national borders.[39] The internet and digital platforms have allowed companies to offer services and products to customers around the world, significantly reducing the costs associated with physical trade and increasing market efficiency.[40] This is particularly beneficial for small and medium sized business which have the opportunity to compete on a global scale without the need for substantial physical infrastructure.

Cross-border data transfers offer numerous benefits, particularly as global connectivity continues to increase and data becomes a critical asset in the digital economy.[41] These transfers allow businesses to operate across borders seamlessly, enhancing productivity and creating new opportunities for innovation and revenue generation.[42] As data is transferred internationally, it supports operations within businesses, between businesses (B2B), between businesses and consumers (B2C), and between machines (M2M), driving global Internet traffic and promoting the expansion of the Internet of Things (IoT).[43]

One major benefit of cross-border data transfers is the ability for manufacturing companies to monitor machines and systems across multiple locations in real-time. For instance, Volkswagen's partnership with Amazon Web Services (AWS) to develop the "industrial cloud" connects data from all machines, plants, and systems in Volkswagen factories globally.[44] Sensors, enabled by cellular or satellite connectivity, send signals that allow for real-time data aggregation at a global level.[45] This not only improves operational efficiency but also enables companies to monetise these insights through new services.

Cross-border data flows provide opportunities for innovation by facilitating international collaboration in research and development (R&D).[46] Access to global datasets helps researchers and companies create new products, improve services, and develop cutting-edge technologies.[47] In fields like healthcare and agriculture, global data sharing has led to significant advancements, such as improved crop yields and the development of more effective vaccines.[48]

39 OECD, Measuring the Economic Value of Data and Cross Border Data Flows, OECD Digital Economy Papers NO 2917 August 2020.
40 Joshua Paul Meltzer, The Internet, Cross Border Data Flows and International Trade 2 (1) Asia & The Pacific Policy Studies.
41 OECD, Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective (OECD Digital Economy Papers, No. 29, August 2020).
42 Ibid.
43 Ibid.
44 Dr Marc Langendorf and Jonas Kulawik, 'Volkswagen and Amazon Web Services to develop Industrial Cloud' (27 March 2019) <Volkswagen and Amazon Web Services to develop Industrial Cloud | Volkswagen Group (volkswagen-group.com)> accessed 16 September 2024.
45 Amazon, 'The Volkswagen Group on AWS' <https://www.volkswagen-group.com/en/press-releases/volkswagen-and-amazon-web-services-to-develop-industrial-cloud-16911> accessed 16 September 2024
46 UNCDF Macmillan Keck, 'The role of cross border flows in the digital economy' (July 2022) <EN-UNCDF-Brief-Cross-Border-Data-Flows-2022 (squarespace.com)> accessed 16 September 2024.
47 Ibid.
48 Ibid.

7.0 Challenges and risks in cross-border data flows

The African Union (AU) Data Policy Framework highlights several challenges and risks to cross-border data flows.[49] First, there is significant concern over the continent's uneven levels of digital readiness.[50] This results in disparities in the ability of member states to implement harmonised policies that foster safe, equitable, and efficient data exchanges.[51]

These challenges are compounded by external pressures from international trade agreements and the global digital economy,[52] which often impose restrictions or standards that do not align with the local context of African nations.[53] As a result, African countries must navigate the fine balance between enabling data flows to foster economic growth and ensuring that local interests, such as data privacy and national security, are protected. Addressing these issues requires a coordinated effort to develop continental-level regulations that support both the free flow of data and the protection of African digital sovereignty.

Indeed, the manifestation of these risks has become evident as in the Worldcoin case in Kenya.[54] The Worldcoin case in Kenya presented significant cross-border data protection risks, particularly concerning the collection and transfer of sensitive personal data, including biometric information such as iris scans.[55] Despite Worldcoin's assertion that it securely stores data on Amazon Web Services in South Africa, the Adhoc Committee raised concerns about the absence of proper safeguards required by Kenya's Data Protection Act 2019 (DPA) for data transfer outside the country.[56] The DPA mandates that data controllers ensure adequate safeguards and the consent of data subjects before transferring sensitive data internationally,[57] but Worldcoin failed to demonstrate compliance with these provisions. Furthermore, the lack of transparency about data storage and deletion mechanisms raises the risk of potential misuse or breaches of personal data, as users were not fully informed about how their biometric data would be managed or its location.[58]

In conclusion, the challenges and risks associated with cross-border data flows in Africa, as highlighted by the African Union Data Policy Framework and illustrated by the Worldcoin case in Kenya, underscore the critical need for data controllers and processors to adhere to stronger data protection laws. As African nations strive to balance the benefits of global

49 AU, 'African Union Data Policy Framework', 41 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed 16 September 2024.
50 Alexander Beyleveld and Franziska Sucker, Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade (SSRN, October 2022) <https://ssrn.com/abstract=4278748> accessed 17 September 2024.
51 Ibid.
52 Ronald Labonté, Trade, Investment and Public Health: Compiling the Evidence, Assembling the Arguments (2019) 15 Globalization and Health <https://doi.org/10.1186/s12992-018-0425-y> accessed 17 September 2024.
53 Ibid. See also Anabel González 'Moving towards a WTO deal on COVID-19 vaccines? (WTO 12 May 2022) <https://www.wto.org/english/blogs_e/ddg_anabel_gonzalez_e/blog_ag_12may22_e.html> accessed 17 September 2024.
54 Florence Ogonjo and Joshua Kitili 'Case commentary on Worldcoin Kenya' (CIPIT, 29 November 2023) <Case Commentary on Worldcoin in Kenya - Centre for Intellectual Property and Information Technology Law (cipit.org)> accessed 17 September 2024
55 Ibid.
56 Ibid.
57 The Data Protection Act (Act No.24 of 2019) eKLR.
58 Worldcoin resumed activities after the probe by the Directorate of Criminal Activities was dropped See Kabui Mwangi 'Worldcoin returns to Kenya after Police dropped investigations' (Business Daily, 20 June 2024) <https://www.businessdailyafrica.com/bd/corporate/companies/worldcoin-returns-to-kenya-after-police-drop-investigations--4664218> accessed 17 September 2024.

digital integration with the protection of local interests, it becomes imperative to establish harmonised regulatory frameworks that ensure data security, privacy, and sovereignty across the continent.

8.0 Domestic Laws on Cross Border Data flows

Regional and domestic frameworks that facilitate cross-border data flows enable the creation of continental and international markets that rely on these flows.[59] Domestic regulations are key in ensuring rights such as privacy, and data protection mechanisms are in place to protect data subjects and ensure that the way in which data is stored, handled and processed is less prone to exploitation.[60] Adequacy decisions are critical for ensuring that data transfers between countries align with both countries' regulations, allowing businesses to seamlessly conduct activities when transferring data internationally.[61] Having domestic regulations is important in ensuring alignment of data protection laws in both countries. It also ensures the existence of a data protection authority to regulate the process in a transparent manner.[62] Such processing is assessed to ensure that effective safeguards are in place and that the recipient country maintains the standards of adequacy.[63]

Building on these regulatory considerations, the Schrems II judgement by the European Court of Justice addressed cross-border data flows between members of the EU and non-members.[64] The Schrems II judgement addressed the importance of adequate data protection laws in countries receiving data from the EU, noting that companies relying on mechanisms like Standard Contractual Clauses (SCCs) must ensure that the data transferred is afforded protections equivalent to EU standards, particularly in the context of cross-border data flows

59 Hanani Hlomani and Caroline B Ncube, 'Data Regulation in Africa: Free Flow of Data, Open Data Regimes and Cybersecurity' (2023) in Data Governance and Policy in Africa, Bitange Ndemo, Njuguna Ndung'u and Abebe Shimeles (eds), Information Technology and Global Governance <https://doi.org/10.1007/978-3-031-24498-8> accessed on 3 October 2024.
60 Andrew D Mitchell and Neha Mishra (n5).
61 Securiti, 'Adequacy Decision' <https://securiti.ai/glossary/adequacy-decision/> accessed on 3 October 2024.
62 Ibid.
63 Ibid
64 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (Schrems II) (Case C-311/18) [2020] ECLI:EU:C:2020:559

to countries like the United States. The Privacy Shield (a mechanism that ensured data flow between members of the EU and the USA) was rendered invalid due to the re-evaluation of theUSA's policies on surveillance to ensure national security.[65] The case also spoke to the validity of standard contractual clauses in transferring data to the USA as affirmed. Factors considered were largely surrounding the legality of both mechanisms.[66] With SCCs being contractual in nature, the individualized way in which cases would be handled differentiated the level of protection from that of the Privacy Shield.[67]

8.1 Overview of domestic laws

Different countries can be classified on a spectrum of being restrictive in the context of cross-border data flows based on the way in which national frameworks are designed. Regulatory approaches range from having no regulations, which results in a lack of restrictions, to ex-post accountability, where individuals can be legally held liable if transferred data is exploited. Conditional flows, the most common approach, involve safeguards that align with data protection and privacy principles, which are essential for successful data transfers. This will be further elaborated in the following section. Finally, ad hoc authorisation is often arbitrary, depending on the standard used for approval and the specific context.[68]

8.1.1 Kenya

Kenya's Data Protection Act addresses the protection of sensitive personal data transferred outside the country through certain safeguards. It requires the consent of a data subject as well as monitoring and regulation by the Data Commissioner to ensure that the rights and freedoms of a data subject are protected.[69] This calls for data controllers and processors to ensure that the right to privacy is not infringed, transparency is upheld and the purpose of processing the data is clear.[70] Section 25(h) further prescribes the need for 'adequate data protection safeguards or consent from the data subject' which essentially calls for explicit consent by the data subject and a sense of uniformity between the regulations of Kenya and that of the other country.[71]

Aspects of data localisation is reflected through the Data Protection Act in that 'grounds of strategic interests of the state or protection of revenue' can be factors to consider for the data centre to be 'located in Kenya'.[72]

Additionally, the Data Protection General Regulations (2021) addresses the transfer of personal data outside Kenya in Part VII. General principles of transfers and efforts to define the scope of 'appropriate safeguards' have been outlined in the same section. The Regulations

65 Sharp Cookie Advisors, 'Schrems II a summary-all you need to know'(2020), <https://www.gdprsummary.com/schrems-ii/> accessed 3 October 2024. In essence, the Schrems II judgment directly invalidated the Privacy Shield, as it was found inadequate in protecting fundamental rights concerning data privacy, which are essential for cross-border data flows under EU law. This ruling significantly impacted how companies handle data transfers between the EU and the U.S., necessitating reliance on other mechanisms like Standard Contractual Clauses (SCCs), with additional safeguards.
66 Ibid.
67 Ibid.
68 OECD, 'Trade and Cross-Border Data Flows' (2021) <Trade and Cross-Border Data Flows> accessed on 18 September 2024.
69 Section 49, The Data Protection Act [Act No. 24 of 2019] Kenya.
70 Section 25, The Data Protection Act [Act No. 24 of 2019] Kenya.
71 Ibid.
72 Section 50, The Data Protection Act [Act No. 24 of 2019] Kenya.

are generally more detailed in nature as compared to the Data Protection Act. While the Act speaks to conditions[73] and safeguards[74] that must be met before transfer of data occurs, the Regulations elaborate on the principles of such transfers[75], their safeguards[76], adequacy of protection[77] subsequent transfers and binding corporate rules[78] among other details that are distinct from the Act.[79]

The Regulations provide for documentation of data transfers to facilitate the notification of the Commissioner in detailing crucial details regarding the type of data transferred, its purpose and basic details.[80] This is compounded by the Commissioner having a public record of the countries that have been deemed to have adequate safeguards.[81]

The Regulations also stipulate conditions to be met in proving the necessity of transferring personal data, including confirmation that the transfer does not infringe on the fundamental rights of the data subject that would outweigh the public interest, and that no international agreements concerning judicial cooperation or police matters are affected.[82]

Exceptions to adequate safeguards are equally outlined in the Regulations, allowing for data transfers in cases where the data subject has explicitly consented, having been informed of the potential risks associated with the transfer. Additionally, the handling of sensitive personal data is specifically addressed under Section 49 of the Data Protection Act.[83]

The scope of the safeguards outlined can be interpreted in a manner that can contextually be more restrictive or less restrictive. In the absence of safeguards, consent becomes key to the transfer.[84] This adds onto the difficulties that tie alongside entities working elsewhere who wish to engage in such data transfer with Kenya.[85]Restriction of data transfers in Kenya therefore is limited to the extent of consent in the case of personal data processed of individuals; however, in the case of data related to the state, the weightage of safeguards significantly steps up, leading to data localisation.

8.1.2 Nigeria

Before the Data Protection Act of Nigeria was enforced, Nigeria National Information Technology Development Agency's Guidelines for Nigerian Content Development in Information and Communications Technology required telecommunication and network service companies to 'host all subscriber and consumer data locally within the country.'[86]

73 Section 48, The Data Protection Act [Act No. 24 of 2019] Kenya.
74 Section 49, The Data Protection Act [Act No. 24 of 2019] Kenya.
75 Regulation 40, The Data Protection (General) Regulations [2021] Kenya.
76 Regulation 41, The Data Protection (General) Regulations [2021] Kenya.
77 Regulation 44, The Data Protection (General) Regulations [2021] Kenya.
78 Regulation 43, The Data Protection (General) Regulations [2021] Kenya.
79 Regulation 47, The Data Protection (General) Regulations [2021] Kenya.
80 Regulation 41(2), The Data Protection (General) Regulations [2021] Kenya.
81 Regulation 44(2), The Data Protection (General) Regulations [2021] Kenya.
82 Regulation 45, The Data Protection (General) Regulations [2021] Kenya.
83 Regulation 46, The Data Protection (General) Regulations [2021] Kenya.
84 Allan Mukuki and Alex Assenga, 'Comparative Study of Data Protection Legislation Frameworks Across the East African Community' (March 2024) <Comparative study of the data protection legislation frameworks across the East African Community> accessed on 18 September 2024.
85 Dan A Kipkoech, 'Africa's Digital Economy: Cross-Border Data Flows under the African Continental Free Trade Area' (CIPIT 31 August 2023) <https://cipit.strathmore.edu/africas-digital-economy-cross-border-data-flows-under-the-african-continental-free-trade-area/>accessed on 18 September 2024.
86 Sections 11.1 (4) and 12.1(4), Guidelines for Nigerian Content Development in Information and Communication Technology (ICT), Nation-

The rationale for this could be the necessity to foster domestic opportunities and thereby employ restrictive measures within data protection laws.[87]

Daigle has collated information concerning the Nigeria Data Protection Regulations (2019), yet again a framework that spoke to data privacy concerns before the Data Protection Act (2023). In defining personal data through ID numbers, location data and other aspects of a person's identity, the ambit of such data had a wide scope. The framework further detailed the protection of sensitive data and granted several rights to subjects such as informed consent, withdrawal of consent and the right to lodge complaints. For data controllers and processors, the NDPR stated that there must be a clear policy and measures to protect data as well as an appointed Data Protection Officer (DPO).

Audits of such practices to ensure compliance were also deemed necessary. Cross-border data transfers were restricted to specific conditions, prioritizing the personal data of subjects.[88] Regulations 2.11 and 2.12 of the NDPR provide for the oversight of the Honourable Attorney General of the Federation (HAGF) to ensure that safeguards in place are catered for by the recipient country including verification of legal safeguards and data protection authorities. Exceptions permitting data transfers may occur when explicit consent from the data subject is obtained, when the transfer is necessary for the performance of a contract, when it serves public interest purposes, or when it is essential for safeguarding the vital interests of the data subject.[89]

Part VIII of the Nigeria Data Protection Act, titled 'cross-border data transfers of personal data,' outlines three sections that examine the validity of such data flows in exceptional circumstances that have legal backing. It further authorises the Nigeria Data Protection Commission to play a central role in the data handling process, involving both the stakeholders and the data itself.[90]

The Data Protection Act thereby safeguards the processing of personal data in the country in line with global standards pertaining to transparency, security and relevant rights. This is with the aim of ensuring potential data privacy risks are catered for despite the mechanisms that are present to facilitate trade and economic growth.[91] Section 41 of the Nigeria Data Protection Act sets strict conditions for transferring personal data from Nigeria to another country. It prohibits such transfers unless the recipient country or entity is governed by laws, contractual agreements, or certification mechanisms that ensure an adequate level of protection.[92] Alternatively, the transfer can occur if specific conditions outlined in Section 43 are met.[93]

al Information Technology Development Agency (2019) <https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf> accessed on 24 September 2024.
87 Mitchell and Mishra, (n48).
88 Brian Daigle, 'Data Protection Laws in Africa: A PanAfrican Survey and Noted Trends' (2021) <https://www.usitc.gov/publications/332/journals/jice_africa_data_protection_laws.pdf> accessed on 24 September 2024.
89 Regulations 2.11 and 2.12, Nigeria Data Protection Regulation [2019].
90 Sections 41, 42 and 43, Nigeria Data Protection Act [2023].
91 Anjayi Philip Muyiwa, 'An Analysis of Nigeria's Legal Framework for Cross-Border Data Transfer: The AfCFTA Perspective'< https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4798172> accessed on 24 September 2024.
92 Section 41, Nigeria Data Protection Act, [2023].
93 Section 43, Nigeria Data Protection Act, [2023].

Additionally, data controllers and processors must document the legal basis for the transfer and ensure that adequate protections are in place.[94] The Commission is empowered to create regulations requiring notification of these measures and their adequacy.[95] It may also impose further restrictions on transferring specific categories of sensitive personal data, depending on the risks to data subjects..[96] Harmony of regulations between that of Nigeria and other countries have been emphasised as necessary despite the associated high costs that could tag along with such restrictions.[97]

8.1.3 Zambia

Part X of the Data Protection Act in Zambia addresses the transfer of data, specifically personal data outside Zambia. Data localisation is provided for in the framework in that such data 'must be stored on a server or data centre located in Zambia' unless authorized by the communications minister.[98] Criticisms with respect to state agencies have been expressed in that they 'could easily access personal data without the consent of data subjects thereby undermining their privacy rights and potentially subjecting them to unauthorized surveillance'.[99]

Sensitive personal data defined under the Act creates an implication of exploitation with respect to fundamental rights and freedoms of the data subject as listed[100] and such data is subjected to data localisation.[101]As is in most countries, consent is key to the transfer of personal data outside the country and overall circumstances surrounding the transfer of data must be considered such as during emergencies.[102] Section 71 of the Data Protection Act outlines the conditions necessary for protecting personal data transferred from Zambia.[103]

The section sets out the conditions under which personal data, excluding sensitive categories, can be transferred outside the Republic. It requires that the data subject consents to the transfer, and that it follows either standard contracts or intra-group schemes approved by the Data Protection Commissioner, or regulations set by the Minister.[104] The Minister is also empowered to issue rules for cross-border transfers, ensuring that adequate data protection and law enforcement mechanisms are in place in the receiving country.[105]

The Data Protection Commissioner is tasked with monitoring these transfers to ensure compliance.[106] There are exceptions where data can be transferred without following the

94 Section 41 (2), Nigeria Data Protection Act, [2023].
95 Section 41 (3), Nigeria Data protection Act [2023].
96 Section 41 (4), Nigeria Data Protection Act, [2023].
97 Dan Allan Kipkoech (n93).
98 Section 70, The Data Protection Act [Act No.3 of 2021] Zambia.
99Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 'Insights into Zambia's Data Protection Act 2021' (2021) <https://cipesa.org/wp-content/files/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf> accessed on 24 September 2024.
100 Section 2, The Data Protection Act [Act No.3 of 2021] Zambia.
101 Section 70, The Data Protection Act [Act No.3 of 2021] Zambia.
102 Section 71 (4), The Data Protection Act [Act No.3 of 2021] Zambia.
103 Section 71 (6), The Data Protection Act [Act No.3 of 2021] Zambia.
104 Section 71 (1) (a) (b), The Data Protection Act [Act No.3 of 2021] Zambia.
105 Section 71 (2), The Data Protection Act [Act No.3 of 2021] Zambia.
106 Section 71 (3), The Data Protection Act [Act No.3 of 2021] Zambia.

standard rules, such as in emergencies related to health services, with explicit consent for sensitive data, or to organisations or countries that meet data protection standards, where the Commissioner determines it necessary.[107] Additionally, the Commissioner must approve standard contracts or intra-group schemes for transfers, these must effectively protect the rights of data subjects.[108]

The feasibility of implementing data localisation in such contexts is questionable, particularly regarding the infrastructure development that may be necessary for foreign entities.[109]

8.1.4 Botswana

The Botswana Data Protection Act (DPA) addresses the trans-border flow of personal data and the transfer of personal data to a third country. Similarly to Nigeria, an exception for the transfer of personal data must be initiated through the Ministry via a Gazette.[110] However, exceptions to the bar set have been provided to ensure that adequate safeguards are in place in the receiving country. Considerations made in such exceptions include the nature of the data being transferred, the purpose and duration of the processing as well as the legal implications surrounding the countries involved.[111]

Further to this, exceptions are provided when the data subject consents to the transfer, when the transfer is necessary for the performance of a contract between the data subject and the controller (including pre-contractual measures requested by the subject), and when it involves the conclusion of contracts between said parties and a third party. Transfers made in the public interest, in the vital interest of the data subject, or when the data is sourced from a public register for public inspection also fall under this ambit.[112]

Such exceptions raise questions about the validity of the complete bar established in Section 48 of the Act. However, they still hold significant weight in preventing several entities from transferring data outside the scope of the aforementioned exceptions. There is, however, scepticism regarding the Minister's discretion in determining whether an exception can be granted.[113]

8.1.5 South Africa

The Protection of Personal Information Act (POPIA) explicitly bars the transfer of data beyond South Africa unless the recipient is subject to a law, binding corporate rules, or a binding agreement that provides an adequate level of protection. This protection must uphold principles of reasonable data processing, and the transfer must meet one of the following

107 Section 71 (4) (a), (b), (c), The Data protection Act [Act No.3 of 2021] Zambia.
108 Section 70 (5), The Data Protection Act [Act No.3 of 2021] Zambia.
109 Dan Allan Kipkoech (n93).
110 Section 48, The Data Protection [Act No.32 of 2018] Botswana.
111 Section 49 (2), The Data Protection [Act No.32 of 2018] Botswana.
112 Section 49(5), The Data Protection [Act No.32 of 2018] Botswana.
113 Kipkoech (n93).

conditions: consent from the data subject, necessity for the performance or conclusion of a contract between the data subject and a third party, or benefit to the data subject.[114] Such 'restrictive' measures have been described to have effects regarding increased costs and reduced efficiency of organisations due to the technological requirements and uncollated data respectively.[115]

Consent in this context extends to the right to withdraw consent and involves an understanding of the associated risks to transferring data to countries that do not meet the adequate safeguards.[116] Section 4.3 of the proposed Code of Conduct for Research (CCR) provides for trans-border information flows and outlines requirements that mirror POPIA including countries in the EU or those that maintain high data protection standards. It further emphasises the necessity of a data transfer agreement for compliance purposes and mirrors other factors related to the alignment of regulations of the receiving country, benefits to the data subject, and more, as outlined in POPIA.[117]

However, its potential application has been critiqued with regards to 'interpretive depth' and recommendations pointing to defining 'transfer of personal information,' scope of adequacy, consent as a legal mechanism as well as defining the people subjected to receiving such data and the overall legalities to such transfer have been expressed.[118]

In similar light, the National Data and Cloud Policy (NDCP), aligned with POPIA, is established with similar aims regarding personal data privacy and compliance with international standards, while the balancing autonomy of South Africa's systems and stakeholders to ensure national security and interests.[119] 'Data-sharing arrangements' with other countries or entities were identified as a point of concern. A set of criteria was established, prioritising national interests, compliance with domestic data protection and security laws, mutual benefits, and the impact of bloc-based regulations concerning cross-border data transfers in a subsequent section.[120] The NDCP is connoted to have links to localisation by suggesting that 'data produced by state entities must be stored in a secure High-Performance Computing and Data Processing Centre' and that it must adhere to regulations set out by the Ministry.

8.1.6 Eswatini

The Data Protection Act of Eswatini is established with the aim of regulating the processing and protection of personal data whilst balancing the right to privacy among other principles such as economic growth.[121] Sensitive personal data is generally bound by restrictive

114 Section 72, Protection of Personal Information Act [2013].
115 Kipkoech (n93).
116 L. Abdulrauf, A. Adaji and H. Ojibara, 'Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the draft Code of Conduct for Research' (2024) 17(1), <https://journals.co.za/doi/full/10.7196/SAJBL.2024.v17i1.1696#:~:text=According%20to%20the%20POPIA%2C%20although,of%20POPIA%20(section%2058).> accessed on 24 September 2024.
117 Section 4.3.9 Code of Conduct for Research [2023].
118 Abdulrauf, Adaji and Ojibara, (n116).
119 Daniel Pretorius and Sinenhlanhla Dlamini, 'South Africa: Data protection considerations in the National Policy on Data and Cloud, 2024' (2024) <https://bowmanslaw.com/insights/south-africa-data-protection-considerations-in-the-national-policy-on-data-and-cloud-2024/> accessed on 24 September 2024.
120 Section 15.4.3, National Policy on Data and Cloud [2024].
121 Melody Musoni, 'Eswatini: An overview of the Data Protection Act' (2022) < Eswatini: An overview of the Data Protection Act | Insights |

measures especially when risks are associated with the processing of the data subject's personal information such as racial or ethnic origin, gender, health and other sensitive information.[122]

The South African Development Community member states have established principles that enable cross border data flows within the region. Eswatini being part of the SADC, has regulations that are preferential to member states.[123] Transfer of data to non-member states of the SADC is permissible provided that adequate safeguards are in place and the purpose of transfer is to 'permit processing'.[124] Particular factors such as 'nature of the data, the purpose and duration of the proposed processing, the country of the recipient, the relevant laws in force in the third country and the professional rules and security measures that are compiled with in that country, have been emphasized further through the framework.[125] Informed consent as well as necessity with respect to (pre) contractual obligations is also addressed within the framework.[126]

The classification of countries that can engage in cross-border data flows into (non) SADC members has been described as a restrictive measure in creating qualifiers depending on the bloc. This alongside other measures may cause the country's stance to be shrouded as restrictive in nature.[127] Other provisions related to cross-border data flows that the country has adopted include the COMESA Simplified Trade Regime (STR) and Trade and Transportation Facilitation instruments for Small-Scale Cross Border Traders (SSCBT) to mitigate a key limitation regarding the extent of small-scale business involvement in cross-border trade[128]

8.1.7 Somalia

In similar light to aforementioned countries, the Data Protection Act of Somalia considers adequate safeguards crucial for the transfer of personal data to a country or international organization, both in terms of protection and regulation, or rather by applicable rules/ principles. Factors considered also extend to the level of access by public authorities in the receiving country, the presence of a data protection authority or officer, as well as their international standing.[129]

In the absence of adequacy, the transfer of data should be justified by demonstrating necessity. This can be done through the data subject's informed consent, with a clear understanding of the risks involved, the necessity of entering into or performing a contract,

DataGuidance> accessed on 24 September 2024.
122 Melody Musoni, 'Africa: The state of cross-border transfer of personal data in the SADC region' (2022) < Africa: The state of cross-border transfer of personal data in the SADC region | Insights | DataGuidance> accessed on 24 September 2024.
123 Ibid.
124 Ibid.
125 Section 33(2), The Data Protection [Act No.5 of 2022].
126 Section 33, The Data Protection [Act No.5 of 2022].
127 Kipkoech (n93).
128 Willis Osemo 'Eswatini has Developed Trade Facilitation Instruments for Small Scale Border Traders' (2020) <Eswatini has Developed Trade Facilitation Instruments for Small Scale Border Traders > accessed on 24 September 2024.
129 Article 30, Data Protection Act [Act No.005 of 2023].

or if the transfer explicitly serves the interests and benefits of the data subject.[130]

Further exceptions are allowed in cases where the data transfer is not repetitive, involves only a limited number of data subjects, is necessary for pursuing compelling legitimate interests of the data controller that do not outweigh the rights and freedoms of the data subject, and where the data controller has assessed the circumstances and implemented appropriate safeguards to ensure personal data protection. Additional exceptions are provided in contexts where data is transferred infrequently to a small number of people. The data controller may assert legitimate interests in transferring the data provided that this does not infringe upon the rights and freedoms of the data subject. Procedurally, the data controller must ensure that appropriate safeguards are in place to protect the data and that both the data protection authority and data subject are aware of such transfer including the reasons behind it. [131]

While informed consent is crucial under the provisions of the Data Protection Act of Somalia, the framework does not prescribe data localisation, as it does not specifically address the storage of personal data outside the country.[132]

8.1.8 Malawi

Section 38 of the Data Protection Act of Malawi stipulates that data transfer from Malawi to another country or international organization is prohibited unless the recipient is subject to a law, binding corporate rules, personal data protection contractual clauses, a code of conduct, or a certification mechanism that ensures an adequate level of protection for personal data.[133]

Adequacy of protection is at the core of data transfers beyond the country and elements to define this factor include consent, necessity to perform a contractual obligation, necessity to perform or conclude a contract or an outright benefit to the data subject.[134] Assessing the adequacy of safeguards has been outlined as an initiation by application or through a data controller/authority so long as fundamental principles such as the rule of law and fundamental rights and freedoms are complied with.[135]

130 Article 31 (1), Data Protection Act [Act No.005 of 2023].
131 Article 31 (3), Data Protection Act [Act No.005 of 2023].
132 Allan Mukuki and Alex Assenga (n 84).
133 Section 38, Data Protection Act [Act No. 3 of 2024] Malawi.
134 Section 39, Data Protection Act [Act No. 3 of 2024] Malawi.
135 Calvin Mulindwa, 'Review of the Malawi Data Protection Act 2024' (CIPIT,25 June 2024) <Review of the Malawi Data Protection Act 2024> accessed 24 September 2024.

9.0 Overview of data protection authorities (DPAs) and their roles

Data protection authorities are entities mandated with the responsibility to apply domestic and international regulations concerning the protection of personal data, investigations relating to wrongful data processing (thereby powers of intervention), engagement in legal proceedings or legal claims by persons/entities as well as report their activities.[136] As such, the functions characteristic to Data Protection Authorities can be summarized into three main categories-advocacy, mediation and enforcement. They apply the laws set forth for data protection and raise awareness regarding the provisions of the law, resolve any disputes that arise and issue binding decisions stemming from such functions.[137] Such entities often are instrumental in enforcing a country's cross-border data flow regulation so as to enable the transfer of data internationally.[138]

Beyond Africa, the General Data Protection Regulation (GDPR plays a crucial role in shaping data privacy laws applicable to the EU and its affiliates, providing a comprehensive framework for the protection and processing of personal and sensitive data. The EU data protection law includes a cross-border restriction on conditions including protection of personal data of natural persons and compliance by the receiving country to 'adequate level of protection' so as to ensure that data can flow freely in a secure manner.[139] Chapters 5 and 6 of the GDPR are instrumental in setting out the transfer of personal data to third countries/international organisations and supervisory authorities.[140]

Professors Cliza and Negura summarize the responsibilities of DPAs in the context of the GDPR through eight major points.[141] These responsibilities include overseeing audits of data processing, organizing awareness programs to educate stakeholders and the general public as to the GDPR's prescriptions and breaches, ensuring that updated policies are notified to the public, managing data subject access requests, managing breaches, facilitating the exercise of data subjects' rights and ensuring compliance on both the public body level and data protection officer level.[142]

Article 11 of the Malabo Convention states that each state 'shall establish an authority in charge of protecting personal data' of independent standing.[143] Further to this, Article 14(6)(b) of the Malabo Convention speaks to the authorization requirement that a data controller must comply with to enable transfer of data via the national data protection authority.[144]

136 Andras Jori, 'Shaping vs Applying Data Protection Law: Two Core Functions of Data Protection Authorities' (2015) 5(2) International Data Privacy Law], <https://doi.org/10.1093/idpl/ipv006>, accessed on 2 August 2024.
137 Ibid.
138 Christopher Kuner, 'Regulation of Trans border Data Flows under Data Protection and Privacy Law: Past, Present and Future' Paper No. 187, (2011) <https://doi.org/10.1787/5kg0s2fk315f-en.> accessed on 18 September 2024.
139 W. Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29 Washington International Law Journal, <https://ssrn.com/abstract=3629348>, accessed on 2 August 2024.
140 General Data Protection Regulation [2016] OJ L 119.
141 Marta-Claudia Cliza and Laura-Cristiana Spataru-Negura, 'The General Data Protection Regulation: What Do Public Authorities and Bodies Need to Know and Do? The Rise of the Data Protection Officer' (2018) 8(2) Juridical Tribune <http://www.tribunajuridica.eu/arhiva/An8v2/12.%20Spataru-Negura,%20Cliza%20EN.pdf> accessed 14 October 2024.
142 Ibid.
143 AU, African Union on Cyber Security and Personal Data Protection <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed on 18 September 2024.
144 AU, African Union on Cyber Security and Personal Data Protection <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed on 23 September 2024.

Similarly, the Economic Community of West African States (ECOWAS) further states that DPAs 'must be composed of qualified persons in the field of law, information communication technology and any other field of knowledge' with regard to the competence of such Authorities in the region.[145] Such characteristics of DPAs are similarly mirrored in the Data Protection Act of Kenya[146], the South African Development Community (SADC) Model Law on Data Protection[147], Protection of Personal Information Act (POPIA) of South Africa[148], the Nigerian Data Protection Act[149], Mauritius Data Protection Act[150] among other national frameworks.

Notably, section 49 of the Kenyan framework speaks to the safeguards in place for cross-border data flows. It prescribes certain duties that the Data Commissioner must fulfil including assessing the interests involved in the transfer and protection of the rights and freedoms of the data subject.[151] Further to this, section 50 alludes to the state's intervention in ensuring the protection of processing data transfers through an entity within the country (a server or a data centre located in Kenya).[152]

Additionally, section 72 of the POPIA regulates cross-border data flows in South Africa. In processing such information, a party is obligated to obtain prior authorization from the Information Regulator (as established in section 39 of the Act).[153] Section 58 of the POPIA further speaks to the authorization process in terms of notification, investigations with specified periods and the issuance of a statement attesting to the legality of such processing.[154] This is evidentiary of the necessity to comply with the Regulator's requirements in facilitating cross-border data flows.

Further, section 41 of the Nigerian framework stipulates that the transfer of personal data outside the country may occur only when the Commission (the Nigerian Data Protection Authority) establishes regulations requiring data controllers and processors to notify and demonstrate the level of protection complied with[155] or when the DPA prescribes for certain types of personal data with distinct procedures.[156] Section 42 addresses the assessment of the adequacy of protection through the Commission and authorizes it to approve any motions brought before them.[157]

Similarly, the Mauritius Data Protection Act provides that the Commissioner (head of the Data Protection Office) must be provided with sufficient information regarding the transfer of personal data outside Mauritius with appropriate safeguards.[158] The Commissioner also reserves the right to request a person to prove that the safeguards provided are sufficient in

145 Article 15, Supplementary Act on Personal Data Protection within ECOWAS [2010].
146 Sections 6(3) and 8(f) and (3), The Data Protection Act [Act No. 24 of 2019] Kenya.
147 Section 3, SADC Model Law on Data Protection [2013].
148 Section 39 (b) and (c), Protection of Personal Information Act [2013].
149 Section 4, Nigeria Data Protection Act, [2013].
150 Section 4(2), Data Protection Act [2017] Mauritius.
151 Sections 49(2) and (3), The Data Protection Act [Act No. 24 of 2019] Kenya.
152 Sections 50, The Data Protection Act [Act No. 24 of 2019] Kenya.
153 Section 57(1)(d), Protection of Personal Information Act [2013].
154 Section 58, Protection of Personal Information Act [2013].
155 Section 41(3), Nigeria Data Protection Act [2023].
156 Section 41(4), Nigeria Data Protection Act [2023].
157 Section 42, Nigeria Data Protection Act [2023].
158 Section 36 (1) (a), Data Protection Act [2017] Mauritius.

protecting their rights and freedoms.[159]

Therefore, regulations across Africa also reflect the principles established by frameworks such as the GDPR, encouraging states to establish Data Protection Authorities (DPAs) as central entities responsible for applying and enforcing laws within their respective jurisdictions.

10.0 Role of Free Trade Agreements and Economic Partnerships in Facilitating Cross-Border Data Flows

10.1 General impact of FTAs on data flows

Free trade agreements (FTAs) play a significant role in facilitating cross-border data flows by providing a structured framework that encourages the free movement of data across borders while addressing regulatory and policy differences. The United States has been a key proponent of this approach, advocating for the "maximum possible free flow of cross-border information" and incorporating specific provisions related to data flows in its trade agreements.[160] For instance, the Free Trade Agreement between the United States and South

159 Section 36 (4), Data Protection Act [2017] Mauritius.
160 See Article 19.11 and 19.12 of the United States, Mexico, Canada Agreement. Article 19.11 provides Article 19.11 prohibits parties from restricting cross-border electronic transfers of information, including personal data, for business purposes. However, parties may implement measures that restrict such transfers if they are necessary to achieve legitimate public policy objectives. These measures must

Korea, effective since 2012, includes clauses that encourage the free flow of information, highlighting the importance of minimising unnecessary barriers to electronic information flows across borders.[161] This emphasis on data flow is also evident in the Trans-Pacific Partnership (TPP) and its successor, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which include binding commitments on cross-border data transfers and restrictions on forced localisation of computing facilities.[162]

In contrast to the United States' approach, the European Union (EU) has prioritised the protection of personal data through regulations like the General Data Protection Regulation (GDPR). The EU's trade agreements, such as the Economic Partnership Agreement with Japan, reflect this balance by including provisions that promote data flow while safeguarding personal data protection.[163] The EU's proposal for cross-border data flows in digital trade agreements emphasises the prohibition of data localisation requirements and supports high standards of personal data protection to build trust and promote trade development.[164] These differing approaches highlight the complexity of negotiating FTAs that involve data flow provisions, as they must reconcile commercial interests with privacy and security concerns.[165]

The World Trade Organization (WTO) currently lacks a comprehensive framework specifically designed to govern cross-border data flows, leading to significant challenges in establishing consistent international rules. The existing WTO agreements, such as the General Agreement on Trade in Services (GATS), include provisions that could be interpreted to cover data flows, but these were crafted in a pre-internet era and do not directly address the unique challenges posed by modern digital trade.[166] For example, GATS Article 5(c) obliges member states to allow the use of public telecommunications networks for the movement of information across borders, yet this does not explicitly cover the nuances of digital data flows.[167]

Efforts to develop a coherent international framework under the WTO have faced slow progress and significant hurdles. The WTO's Joint Statement Initiative (JSI) on Electronic Commerce, launched in 2019, aims to create new rules for digital trade, including data flows.[168] However, achieving consensus among WTO members has been difficult due to divergent national interests and policy preferences.[169] The fragmented nature of current international regulations and the strong influence of powerful economies on trade rules have further complicated the creation of a unified template for cross-border data flows under the WTO.

not be discriminatory, unjustifiably restrictive on trade, or impose more restrictions than necessary to meet the policy objective and Article 19.12 prohibits parties from requiring businesses to establish or use computing facilities within their territory as a condition for conducting business. <19-Digital-Trade.pdf (ustr.gov)>

161 See Article 12.4 and 12.5, KORUS FTA <COVER PAGE (ustr.gov)> accessed 2 July 2024.

162 Yik-Chan Chin and Jingwu Zhao, 'Governing Cross-Border Data Flows: International Trade Agreements and Their Limits' (2022) 11 Laws 63 https://doi.org/10.3390/laws11040063 accessed 5 July 2024.

163 See Article 8.63 on Transfers of Information and Processing of Information <CL2018A1227EN0020010.0001.3bi_cp 1..1 (europa.eu)> accessed on 4 July 2024.

164 Ibid.

165 Yik-Chan Chin and Jingwu Zhao (n 162).

166 Czar Matthew Gerard T. Dayday, 'Cross-Border Data Flows and Data Regulation under International Trade Law' (2023) 96 Phil LJ 33 -81.

167 Section 5 c of the Annex on Telecommunications of the General Agreement on Trade in Services, <26-gats.wpf (wto.org)> accessed on 4 July 2024.

168 Joint Statement Initiative on Electronic Commerce <E-Commerce Plurilateral - WTO Plurilaterals Info> accessed on 5 July 2024.

169 Czar Matthew Gerard T. Dayday, 'Cross-Border Data Flows and Data Regulation under International Trade Law' (2023) 96 Phil LJ 65 -67.

When negotiating trade agreements involving superpowers, smaller and developing countries may have to accommodate the interests of these powerful nations to secure favourable trade terms.[170] This accommodation can lead to significant sacrifices in policy space, as seen in the inclusion of stringent data flow provisions in agreements led by the United States.[171] The US's focus on ensuring the free flow of data as a core norm in its trade agreements often translates into demands for minimal restrictions on data transfers and prohibitions on data localisation measures. These provisions can constrain the ability of other countries to implement their own data protection and localisation policies, thus limiting their regulatory autonomy.[172]

The following section delves into free trade agreements and partnerships, examining their role in shaping the regulatory frameworks governing cross-border data flows.

10.2 Kenya-UK Economic Partnership Agreement

The Economic Partnership Agreement (EPA) between the Republic of Kenya and the United Kingdom of Great Britain and Northern Ireland (Kenya-UK EPA), signed on 8th December 2020, sets out to maintain and enhance trade relations between the two countries following the UK's departure from the European Union.[173] This agreement is intended to ensure continuity and certainty of trade relations, facilitating duty-free and quota-free access for Kenyan goods into the UK market and gradually liberalising access for UK goods into Kenya.[174] The EPA aims to promote sustainable growth and poverty reduction in Kenya by fostering increased trade and investment, supporting Kenya's development goals.

However, the EPA has faced criticism for the lack of public participation and transparency in its negotiation and ratification process.[175] Civil society organisations and some members of the Kenyan parliament have raised concerns about the potential negative impact on local industries and regional trade dynamics.[176] They argue that the agreement might benefit UK companies more than Kenyan industries, particularly by opening the Kenyan market to high-value UK products while Kenya primarily exports low-value agricultural products.

Article 10 of the 2nd Protocol of the Agreement, titled Mutual Assistance in Customs Matters has provisions that outline how cross-border data flows are to be governed.[177] Firstly, any

170 Harrison Mbori and James Thuo Gathii, 'Bilateralizing the EU-EAC EPA: An Introductory Legal Analysis of the Kenya-UK Economic Partnership Agreement' (Afronomicslaw, 26 February 2020) <https://www.afronomicslaw.org/analysis/bilateralizing-the-eu-eac-epa-an-introductory-legal-analysis-of-the-kenya-uk-economic-partnership-agreement> accessed 5 July 2024.
171 Yik-Chan Chin and Jingwu Zhao (n 162).
172 Calvin Mulindwa, 'Negotiating Digital Frontiers: The United States Kenya STIP and the Future of Cross-Border Data Flows' (CIPIT, 13 June 2024) <Negotiating Digital Frontiers: The United States Kenya STIP and the Future of Cross-Border Data Flows - Centre for Intellectual Property and Information Technology law (strathmore.edu)> accessed 5 July 2024.
173 Claire Brader, 'UK - Kenya Economic Partnership Agreement (Brexit & the EU, Foreign Policy, (International Trade, 26 February 2021) <UK-Kenya Economic Partnership Agreement - House of Lords Library (parliament.uk)> accessed 5 July 2024.
174 Ibid.
175 Harrison Mbori and James Thuo Gathii, 'Bilateralizing the EU-EAC EPA: An Introductory Legal Analysis of the Kenya-UK Economic Partnership Agreement' (Afronomicslaw, 26 February 2020) <https://www.afronomicslaw.org/analysis/bilateralizing-the-eu-eac-epa-an-introductory-legal-analysis-of-the-kenya-uk-economic-partnership-agreement> accessed 5 July 2024.
176 Ibid.
177 See the Article 10 of the Second Protocol <CP 339 – Economic Partnership Agreement between the United Kingdom of Great Britain and Northern Ireland, of the one part, and the Republic of Kenya, a Member of the East African Community, of the other part (publishing.service.gov.uk)> accessed on 5 July 2024.

information communicated under this protocol is to be treated as confidential or restricted in accordance with the applicable rules of each Party involved.[178] This information will be subject to official secrecy obligations and will receive the same level of protection as similar information under the laws of the receiving Party.[179] This ensures that sensitive information remains secure and protected against unauthorised access or disclosure.

Secondly, the exchange of personal data is contingent upon the receiving Party's commitment to ensuring an adequate level of protection.[180] The protection must be equivalent to the standards applied by the Party supplying the data.[181] To facilitate this, the Parties are required to share information regarding their respective data protection rules and legal provisions.[182] This mutual communication helps to harmonise data protection measures, ensuring that personal data is safeguarded consistently across jurisdictions.

These provisions collectively underscore the importance of robust data protection frameworks in managing cross-border data flows. By mandating equivalent levels of data protection and emphasising the confidentiality of exchanged information, the protocol aims to foster a secure and reliable environment for international data exchanges.

10.3 US-Kenya Strategic Trade and Investment Partnership (ongoing)

The US-Kenya Strategic Trade Investment Partnership (STIP) is still being negotiated. The sixth round of negotiations took place from June 3 to 7, 2024, in Mombasa, Kenya. The US-Kenya STIP aims to increase investment, promote sustainable and inclusive economic growth, benefit workers, consumers, and businesses (including micro-, small-, and medium-sized enterprises), and support African regional economic integration.[183]

The U.S. Trade Representative has not yet released a summary of the texts submitted for the chapter on digital trade. However, an educated inference regarding the contents of this chapter can be drawn from the provisions included in previously concluded free trade agreements involving the United States.

The United States has consistently prioritised commercial interests and market access in its digital trade agreements with other nations. This policy orientation was notably articulated during the Clinton administration, which championed the principle of the 'maximum possible free flow of cross-border information'.[184] This stance was intended to ensure that regulatory differences between nations do not morph into significant barriers to trade.

In 2002, the US proposed the Digital Agenda to promote the liberal flow of cross-border data through bilateral and regional trade agreements.[185] US-led agreements tend to focus on the

178 Ibid Article 10.1.
179 Ibid Article 10.2.
180 Ibid Article 10.2.
181 Ibid Article 10.2.
182 Ibid Article 10.2.
183 Office of the United States Trade Representative <United States and Kenya Announce the Launch of the U.S.-Kenya Strategic Trade and Investment Partnership | United States Trade Representative (ustr.gov)> accessed on 8 July 2024.
184 White House, A Framework for Global Electronic Commerce, 1 July 1997.
185 Yik-Chan Chin and Jingwu Zhao (n 162).

freedom of choice of individuals in digital products and services and the restriction of data localisation requirements.[186]

In 2016, the US led the negotiations for the Trans-Pacific Partnership Agreement (TPP). It was the first time the USA made a binding commitment to free cross-border data flow.[187] Chapter 14 committed each TPP government to permit cross-border transfer of information, including personal and business information, by electronic means on condition the activity is for the business of a covered person.[188] It also allowed a government to maintain data localisation requirements on condition that it was necessary to achieve a public policy objective.

In 2017, the United States-Mexico-Canada Agreement was negotiated by the three countries to replace the North American Free Trade Agreement (NAFTA). The Agreement creates an avenue for the expansion of trade and investment in innovative products and services, a field where the US has a competitive advantage.[189] This Agreement laid a stronger emphasis on favouring cross-border data flows to enable digital commerce, prohibiting parties from restricting cross-border transfer of information and restricting companies from using or locating computing facilities in a party territory for conducting business.[190]

American corporations have maintained the same view and advised the government to adopt the same provisions as the United States-Mexico-Canada Agreement in the coming US-Kenya STIP. For example, PhRMA, IBM, and The App Association all opposed the prohibition of cross-border data flows rationalising them as barriers to trade.[191] Similarly, for data localisation requirements, they advise that the agreement should discourage data localisation requirements to allow better market access and reduce operating costs.

10.4 Tripartite Free Trade Area (TFTA) and its current status

The TFTA was agreed upon by the member states of COMESA, EAC, and SADC in October 2008.[192] It encompasses 29 countries representing 53% of the African Union's membership. The TFTA's primary objectives are to promote economic and social development, create a large single market with free movement of goods and services, enhance regional and continental integration and build a strong free trade area.[193]

The TFTA officially came into force on 25 July 2024, after reaching the required threshold of 14 ratifications with Angola being the latest to ratify on 25 June 2024.[194] While it does not explicitly mention cross-border data flows in its provisions, it focuses on fostering

186 See Digital Trade Chapter of the Comprehensive Agreement for Trans-Pacific Partnerships (CPTPP) and the United States Mexico (USMACA).
187 Trans-Pacific Partnership, < Trans-Pacific Partnership: Summary of U.S. Objectives | United States Trade Representative (ustr.gov)> accessed on 6 March 2024. Kindly note that the USA withdrew from negotiations in 2017. And the Comprehensive and Progressive Agreement for Trans-Pacific Partnership was created.
188 Chapter 14: Electronic Commerce, < Trans-Pacific Partnership: Summary of U.S. Objectives | United States Trade Representative (ustr.gov)> accessed on 6 March 2024.
189 Article 19.11, The United Sates-Mexico-Canada Agreement < 19-Digital-Trade.pdf (ustr.gov)> accessed on 24 January 2024.
190 Article 19.11, The United Sates-Mexico-Canada Agreement < 19-Digital-Trade.pdf (ustr.gov)> accessed on 24 January 2024.
191 CIPIT < theuskenyaftainsights.org/media/1989674354.pdf> accessed on 29 April 2024.
192 tralac <COMESA-EAC-SADC Tripartite FTA - tralac trade law centre> accessed on 29 July 2024.
193 Article 4, Agreement Establishing a Tripartite Free Trade Area among COMESA, EAC and SADC.
194 COMESA, <COMESA-EAC-SADC Tripartite Free Trade Area Comes into Force – Common Market for Eastern and Southern Africa (COMESA)> accessed on 12 August 2024.

cooperation in the harmonisation of data management practices among member states.[195]

This reflects the trend within African regional economic communities, where there is an uneven approach to regulating cross-border data flows. The EAC for example emphasizes the need for harmonisation to facilitate data flow, especially in the context of e-commerce and digital services.[196] The East African Community E-commerce Strategy notes that data localisation and sovereignty derail the free flow of data within the EAC. The Strategy calls for adoption of best practices, including the ratification of the Malabo Convention and adoption of the United Nations Conference on Trade and Development (UNCTAD) Cyber law Framework.[197]

In SADC, their SADC Customs ICT strategy stresses the need for enhancing connectivity and harmonisation across member states through improved information and communication technology. The Strategy aims to harmonise data exchange and IT connectivity across SADC member states. This involves adopting common customs application systems and using internationally accepted standards, particularly those set by the World Customs Organisation (WCO).[198] The Strategy emphasizes the automation of custom processes and supports the use of ICT to improve transparency, efficiency and security in customs operations. This includes moving towards paperless custom procedures to streamline processes and reduce complexity of cross-border trade.[199] The SADC strategy is geared towards creating a more integrated, efficient and secure customs environment that supports smoother and faster cross-border data flows, which are essential for effective trade facilitation and regional integration.

195 Article 14, Agreement Establishing a Tripartite Free Trade Area among COMESA, EAC and SADC.
196 East African Community, 'East African Community E-commerce Strategy' Adopted by EAC Council on 12th July 2022.
197 Nelly C. Rotich (n12).
198 SADC Customs Information Communication Technology Strategy <Microsoft Word - SADC CUSTOMS ICT STRATEGY> accessed on 12 August 2024.
199 Ibid.

11.0 Data Protection Aspects Relevant to Cross-Border Data Flows

Several Data Protection Acts delineate data protection aspects that must be adhered to when processing or collecting individuals' data.[200] These aspects encompass key principles and considerations vital for ensuring the protection and proper handling of personal data, particularly in the context of cross-border data transfers, as discussed below.

11.1 Consent and Legitimacy

The Kenya Data Protection Act requires a data subject's consent to transfer personal data outside the country.[201] This means individuals must actively agree to their data being processed or transferred internationally, which includes providing a clear and affirmative action indicating consent.[202] The consent must be well informed, specific to the data use purpose and given freely without coercion.

Beyond Kenya, many African countries' data protection frameworks, such as those guided by the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), reflect similar provisions.[203] The Malabo Convention promotes data sovereignty by requiring adequate safeguards for cross-border data transfers, with explicit consent being a critical component to ensure legitimacy.[204] Similarly, the EU's General Data Protection Regulation (GDPR) serves as an international benchmark, enforcing strict consent requirements and applying adequacy decisions for non-EU countries that receive data.[205]

11.2 Purpose Limitation

Several African Data Protection Acts provide that cross-border transfers occur only if the recipient is subject to data protection law, binding corporate rules or an agreement that upholds similar principles for the processing of personal information. Furthermore, data can only be transferred for specific, explicit and legitimate purposes. For example Section 71 of the Data Protection Act of Zambia, provides that transfer of cross border data must be for predefined uses outlined in contracts pre-approved by the Data Protection Commissioner; additionally even in exceptional circumstances, data transfers must align with purpose limitation requirements.[206] Similarly, Section 28 of the Cyber and Data Protection Act of Zimbabwe ensures adherence to the principle of purpose limitation by stipulating that personal data may only be transferred to third parties in foreign countries if those parties provide an adequate level of protection;[207] this is assessed based on the nature of the data,

200 Data Protection Africa <Data Protection Africa | ALT Advisory> accessed on 12 August 2024.
201 Section 49 (1), Data Protection Act, [Act No.24 of 2019]. See also The Protection of Personal Information Act (POPIA) of South Africa and The Personal Data Protection Act of Tanzania.
202 Section 38, Data Protection Act [Act No. 3 of 2024] Malawi.
203 AU, 'African Union on Cyber Security and Personal Data Protection <29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (au.int)> accessed 16 September 2024.
204 Ibid.
205 Article 49 (1) (a) General Data Protection Regulation <General Data Protection Regulation (GDPR) – Legal Text (gdpr-info.eu)> accessed 16 September 2024.s
206 Section 71, The Data Protection Act [Act No.3 of 2021] Zambia.
207 Section 28, Cyber and Data Protection Act 2021[Chapter 12:07] Zimbabwe

its intended use, the duration of its processing and the data protection laws and security measures in place in the recipient's country or organisation. This ensures that the data is used strictly for purposes within the controller's competence and is protected according to high standards aligning with purpose-specific limitations to safeguard data subject rights.

11.3 Transparency and accountability

The principles of transparency and accountability are fundamental in ensuring trust and compliance in cross-border data flows. Transparency requires that individuals are fully informed about how their personal data is collected, used, shared, and transferred across borders, while accountability mandates that organisations handling the data take full responsibility for ensuring its protection and lawful processing.[208]

The requirement to report transfers to the Data Protection Agency, and the rigorous assessment of the recipient country's data protection standards, exemplifies the accountability mechanisms that ensure data is handled responsibly.[209] Transparency is maintained through clear communication with data subjects, especially when explicit consent or specific authorisation is required for transfers to countries with inadequate protections.

Many African Data Protection Acts mandate that for cross-border data flows to occur, there must be an adequate level of protection provided by the recipient.[210] For example, under the Data Protection Law of Angola, the international transfer of data that provide an adequate level of protection is allowed, but it must be reported to the Data Protection Agency.[211] Under the Act a country is considered to provide an adequate level of protection if it guarantees, at minimum a protection level equivalent to that established by Angola.[212]

The adequacy of the data protection level in a recipient state is evaluated by the Data Protection Agency. This assessment is thorough and considers all aspects related to the data transfer such as the nature of data, the purpose and duration of its processing, the rules of law, general or sector specific rules in the recipient country and the security measures enforced there.[213]

However, if a country does not ensure an adequate level of protection of protection, the transfers are then subject to specific conditions and must be authorised by the Data Protection Agency.[214] Authorisation can be granted if conditions such as the data subject's explicit consent, the necessity of the transfer for contractual performance, or legal requirements for the protection of public interest are met.[215]

208 Chisolm Ikezurora, 'Unveiling the Nexus: The Relationship Between Transparency and Accountability in Data Privacy (PRIVACYEND, January 12 2024) < Unveiling the Nexus: The Relationship Between Transparency and Accountability in Data Privacy - PrivacyEnd> accessed on 14 October 2024.
209 See Section 71 (1) (a) (b), The Data Protection Act [Act No.3 of 2021] Zambia; Section 41 (2), Nigeria Data Protection Act, [2023] and Regulation 41(2), The Data Protection (General) Regulations [2021] Kenya.
210 See Section 41 (1) (a), Data Protection Act of Nigeria [2023]; Article 30 (1) of the Somalia Data Protection Act; Section 28 (1) Cyber and Data Protection Act of Zimbabwe; Section 38 of the Data Protection of Malawi; Section 72 of the Protection of Personal Information Act of South Africa and Section 48 (a) and (b) of the Data Protection Act of Kenya.
211 Article 33 Protection of Personal Data [Lei No 22/11] Angola.
212 Ibid.
213 Article 33 (4), Protection of Personal Data [Lei No 22/11] Angola.
214 Article 34, Protection of Personal Data [Lei No 22/11] Angola. See also Section 29 Cyber and Data Protection Act of Zimbabwe; Section 39 (4) of the Data Protection of Malawi; Section 71 (4) of the Zambian Data Protection Act; Article 31 of the Somalia Data Protection Act.
215 Ibid.

11.4 Security and confidentiality

Security and confidentiality are paramount in cross-border data flows, ensuring that sensitive personal and corporate information remains protected during international transfers.[216] As data moves across national boundaries, it is exposed to various risks, including unauthorised access, cyberattacks, and breaches that can lead to significant financial, reputational, and legal consequences.[217] To mitigate these risks, robust security measures such as encryption, secure communication channels, and access controls must be in place to safeguard the data. Encryption, for example, ensures that even if data is intercepted during transfer, it remains unreadable to unauthorised parties. Confidentiality mandates that only authorised individuals or entities have access to the data, maintaining the integrity and privacy of the information.

The AU Data Policy Framework emphasises the need for strong governance mechanisms to enforce these protections, ensuring that both data controllers and processors adhere to strict security protocols when handling cross-border data.[218] This includes implementing measures like data anonymization, audit trails, and regular security assessments to detect and prevent any vulnerabilities in the data transfer process. Additionally, countries often require that foreign data processors and controllers provide equivalent levels of data protection to ensure continuity in confidentiality, regardless of where the data is stored or processed. For example, under the framework, personal data can only be transferred if the recipient country guarantees an adequate level of security, similar to domestic standards.

216 W. Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29 Washington International Law Journal, <https://ssrn.com/abstract=3629348>, accessed on 2 August 2024.
217 Tshilidzi Marwala, Eleonore Fournier-Tombs, and Serge Stinckwich, Regulating Cross-Border Data Flows: Harnessing Safe Data Sharing for Global and Inclusive Artificial Intelligence, Technology Brief No. 3, October 2023 (United Nations University) https://collections.unu.edu/eserv/UNU:9291/UNU-TB_3-2023_Regulating-Cross-Border-Data-Flows.pdf accessed 3 October 2024
218 African union, AU Data Policy Framework, 41 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed 16 September 2024.

12.0 Challenges to Harmonisation of Data Protection Laws

Harmonising data protection laws across African countries presents several challenges, significantly impacting the potential cross-border data flows within the continent. These challenges stem from the diverse and conflicting regulatory frameworks that have been established by various nations to safeguard personal data, driven by varying levels of economic development, legal traditions and concerns over data sovereignty and security.

In this context and informed by the African Union Data Policy Framework 2022, African countries are encouraged to identify and adopt the most appropriate approach to cross border transfers.[219]

12.1 Open Transfers Regime

This regime has minimal mandatory approval requirements and relies on voluntary private sector standards, allowing for the free movement of data.[220] It is most suitable for digital services and data-driven value creation, offering the greatest flexibility in data movement. However, it presents risks, including the proliferation of inconsistent standards across jurisdictions, limited data subject rights, and challenges in monitoring private firms' compliance. Privacy is considered a consumer right under this regime.[221]

12.2 Conditional Transfers Regime

Based on established regulatory data safeguards and guidelines from data protection authorities or international agreements, this regime balances data protection with the need for data transfer for value creation.[222] It emphasizes strong data subject rights and requires certain conditions to be met before data can be transferred.[223] This regime can encourage the establishment of domestic data processing authorities but may lead to increased compliance burdens and potential digital trade bottlenecks.

12.3 Limited Transfer Model

Cross-border data flows are heavily regulated under this model, with government approval and data localisation requirements playing key roles.[224] The focus is on national security and public data control, with stringent regulatory approval required for international data transfers.[225] This regime may involve mandatory data localisation and storage, limiting the global free flow of data and reinforcing national control.

Harmonising data protection laws across Africa faces significant challenges due to the differing political, economic, and regulatory landscapes of various countries. The existence

219 African Union, AU Data Policy Framework pg 42 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed on 19 August 2024. This categorisation can also be named 'free flow', 'flow conditional on safeguards' and 'flow conditional, including ad hoc authorisations' It is important to note that these categorisations do not represent individual countries as different approaches can be applied to different types of data. See Casalini F and J. López González (2019-01-23) 'Trade and Cross Border Data Flows' OECD Trade Policy Papers No.220 OECD Publishing Paris <*b2023a47-en.pdf (oecd-ilibrary.org)> accessed on 19 August 2024.
220 African Union, AU Data Policy Framework pg 42 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed on 19 August 2024.
221 The United States of America adopts this regime; The USA does not have a comprehensive federal data protection law.
222 Ibid.
223 Examples of countries that have adopted this regime: Kenya, Tanzania, Malawi, Somalia, South Africa, Nigeria, The European Union.
224 African Union, AU Data Policy Framework pg 42 <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed on 19 August 2024.
225 China and Russia have adopted limited transfer regimes.

of distinct data transfer regimes—ranging from open to conditional and limited transfer frameworks—reflects the diverse priorities of each nation, shaped by their unique concerns over data sovereignty, national security, and economic development. Countries with stronger regulatory structures and advanced digital economies may favour flexible, market-driven regimes, while others with more cautious stances may adopt stringent, localised controls to protect their national interests. These differing approaches create inconsistencies in legal standards, complicating efforts to establish a unified framework that supports seamless cross-border data flows. Additionally, the varying levels of institutional capacity and political will to implement and enforce such laws further complicate harmonisation efforts, as nations seek to balance economic growth, data privacy, and national security in ways that reflect their specific contexts. Ultimately, these divergences pose significant barriers to creating a harmonised legal environment for data protection across Africa.

13.0 Safeguarding Personal Data in Cross-Border Transfers: The Role of African Data Protection Acts and the AU Data Policy Framework

African states with Data Protection Acts recognise the crucial importance of safeguarding personal data. While cross-border data transfers are permitted, they emphasise that such transfers must be backed by proof that the recipient has adequate safeguards in place to protect data subject rights.[226] These safeguards can include a law, binding corporate rules,[227] a personal data protection contractual clause, a code of conduct, or a certification mechanism, all in compliance with the specific requirements outlined in the relevant data protection legislation.[228]

To illustrate this, the Data Protection Act of Zimbabwe provides that a data controller in Zimbabwe may only transfer personal information to a foreign third party if the recipient country or international organisation provides an adequate level of protection for the data.[229] The adequacy of protection is assessed based on the nature of the data, the purpose and duration of processing, the recipient's legal framework, and security measures.[230] The transfer is permitted solely to fulfil tasks within the data controller's competence.

Overall, African states with Data Protection Acts underscore the necessity of robust safeguards for cross-border data transfers to ensure the protection of personal data. These safeguards can take various forms, including laws, binding corporate rules, or certification mechanisms, in line with data protection legislation.

Ultimately, the African Union under the AU Data Policy Framework is cognisant of the unevenly developed infrastructure across the continent and calls upon states to encourage and support data flows within and between AU Member States by establishing a Cross-Border Data Flows Mechanism that considers varying levels of digital readiness, data maturity, and the legal and regulatory contexts of different countries.[231] Additionally, it promotes data exchange across sectors and borders by creating a Common Data Categorisation and Sharing Framework that addresses the different types of data and their corresponding privacy and security requirements.[232]

226 See Section 31 (2) Personal Data Protection Act [Act No.11 od 2022] Tanzania and Section 48 (a) of the Data Protection Act [Act No. 24 of 2019]. The latter specified this proof must be furnished upon the Data Commission while the latter the Data Protection commissioner.
227 Similarly, under Section 70 (3) The Data Protection [Act No.3 of 2021] Zambia, The Data Protection Commissioner shall approve and certify inter-group schemes for compliance.
228 See Section 38 of the Data Protection Act of Malawi and Article 30 of the Data Protection Act of Somalia.
229 Section 28 (1), Cyber and Data Protection Act [Chapter 12:07] Zimbabwe.
230 Section 28 (2), Cyber and Data Protection Act [Chapter 12:07] Zimbabwe
231 African Union, AU Data Policy Framework <42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf> accessed on 19 August 2024.
232 Ibid.

14.0 Case Studies of Effective Data Protection in Cross-Border Transfer of Data from the EU

The European Union (EU) has consistently demonstrated a strong commitment to protecting the personal data of its citizens, particularly in the context of cross-border data flows. One of the most significant examples of this commitment is the evolution and implementation of the EU-U.S. Privacy Shield Framework, designed to regulate data transfers between the EU and the United States.[233] This framework was developed in response to the inadequacies found in previous mechanisms and serves as a robust case study of how the EU has navigated the complex landscape of cross-border data protection.

The EU's approach to data protection is grounded in the principles set out in the 1995 Data Protection Directive (Directive 95/46/EC),[234] which established that personal data could only be transferred to non-EU countries if they provided an "adequate" level of protection. Initially, this adequacy was deemed to be provided by the U.S. under the Safe Harbour Agreement.[235] However, the Safe Harbour framework came under intense scrutiny, especially after revelations in 2013 concerning the extent of U.S. government surveillance programs.[236] These revelations led to a reassessment of the framework, culminating in the European Court of Justice (ECJ) invalidating the Safe Harbour agreement in 2015 through the landmark Schrems ruling.[237]

Following the invalidation, the EU and the U.S. negotiated a new framework—the EU-U.S. Privacy Shield.[238] The Privacy Shield aimed to address the concerns raised by the ECJ and to ensure that data transferred from the EU to the U.S. would be afforded an "essentially equivalent" level of protection as within the EU.[239]

The Privacy Shield introduced several mechanisms to enhance the protection of EU citizens' data. Notably, it established a framework of principles that U.S. companies had to comply with to self-certify under the Privacy Shield.[240] These principles included robust obligations concerning data integrity, purpose limitation, and transparency, as well as enhanced mechanisms for redress, enforcement, and liability.[241]

One of the central protections under the Privacy Shield was the establishment of the Ombudsperson mechanism.[242] This provided EU citizens with a dedicated channel through which they could raise concerns about potential access to their data by U.S. government agencies.[243] The Ombudsperson, independent of the Intelligence Community, was tasked

233 Privacy Shield Framework <Privacy Shield> accessed 26 August 2024.
234 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
235 Steven Ward, 'The Rise and Fall of the Safe Harbour Privacy Treaty' <https://www.rstreet.org/commentary/the-rise-and-fall-of-the-safe-harbor-privacy-treaty/> accessed on 26 August 2024.
236 Ibid.
237 Case C-362/14 Maximillian Schemes v Data Protection Commissioner EU:C: 2015:650.
238 Privacy Shield Framework <Privacy Shield> accessed 26 August 2024.
239 Ibid.
240 Part III Section 6, Privacy Shield Framework <Privacy Shield> accessed 26 August 2024.
241 Part II, Privacy Shield Framework <Privacy Shield> accessed 26 August 2024.
242 See para 65 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1.
243 Privacy Shield <Microsoft Word - Privacy Shield Framework final 7-6.docx> accessed on 26 August 2024.

with investigating and addressing complaints related to national security access to data.[244]

Moreover, the Privacy Shield also introduced stringent rules around onward transfers of data, ensuring that any data transferred from the U.S. to a third party would maintain the same level of protection.[245] This was critical in preventing data from being transferred to jurisdictions with weaker data protection standards.

Despite its robust framework, the Privacy Shield was not without its risks and challenges. One of the primary risks stemmed from the differing legal frameworks between the EU and the U.S., particularly regarding government access to data for national security purposes.[246] Although the Privacy Shield sought to limit and regulate such access, concerns persisted about the adequacy of these measures, especially given the broad surveillance powers available to U.S. authorities under laws like the Foreign Intelligence Surveillance Act (FISA).[247]

Another challenge was the reliance on self-certification by U.S. companies, which, while accompanied by enforcement mechanisms, raised concerns about the consistency and reliability of compliance.[248] The enforcement was primarily the responsibility of the U.S. Federal Trade Commission (FTC), which was tasked with investigating and addressing non-compliance.[249] However, the effectiveness of these measures was questioned, particularly in light of the growing complexities of data flows in the digital economy.

The experience with the Privacy Shield underscores several nuances in the protection of data in cross-border transfers. First, it highlighted the importance of continuous oversight and review. The EU built in mechanisms for an annual review of the Privacy Shield, during which it could assess the adequacy of protections and ensure that the framework adapted to emerging challenges.

Secondly, the Privacy Shield demonstrated the need for a balanced approach that recognizes the legitimate needs of both data protection and national security. The framework attempted to strike this balance by allowing for data transfers while imposing limitations and safeguards on U.S. authorities' access to that data.

Ultimately, the Privacy Shield was invalidated by the ECJ in July 2020 in the Schrems II ruling, which found that the framework still did not provide sufficient protection against U.S. surveillance.[250] This ruling has led to further negotiations and the development of new frameworks, such as the EU-U.S. Data Privacy Framework, which continues to evolve in response to these challenges.[251]

The EU's approach to data protection in the context of cross-border data transfers, as

244 Ibid.
245 Part III, Section 10 Privacy Shield Framework <Privacy Shield> accessed 26 August 2024.
246 See para 65-77, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1.
247 Ibid.
248 Ana Andrijevic, 'Privacy Shield Challenged a second time' (Diplo 2016) <Privacy Shield challenged a second time - Diplo (diplomacy.edu)> accessed on 26 August 2024.
249 See para 26 -29, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1.
250 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems EU:C:2020:559.
251 European Commission, <EU-US data transfers - European Commission (europa.eu)> accessed 26 August 2024.

exemplified by the Privacy Shield, highlights the complexities and evolving nature of data protection in a globalized world. While the Privacy Shield represented a significant step forward in protecting EU citizens' data, its limitations and eventual invalidation underscore the ongoing need for vigilance, adaptation, and innovation in the face of emerging risks and challenges in cross-border data flows.

15.0 Recommendations for Policymakers and Businesses

15.1 Develop Robust Data Protection Frameworks

Policymakers across Africa must prioritize the establishment of comprehensive data protection laws that align with international standards. While some African countries have made significant strides, others lag in implementing robust data governance frameworks. Harmonisation of these laws across the continent would facilitate smoother cross-border data flows and support economic integration. Policymakers should consider adopting frameworks that balance the need for data protection with economic growth, ensuring that local businesses are not overly burdened by compliance requirements. Incorporating key elements such as data minimization, purpose limitation, consent and legitimacy is essential for creating a reliable data environment.

15.2 Encourage Regional Cooperation and Harmonisation

The diverse regulatory frameworks across Africa present significant challenges to cross-border data flows. To address this, regional bodies like the African Union should spearhead efforts to harmonize data protection laws. This harmonisation would reduce the friction in data transfers and provide a consistent legal environment for businesses operating across multiple countries. Furthermore, harmonized regulations would attract foreign investment by offering predictable and secure data processing conditions.

15.3 Leverage Technological Infrastructure

Policymakers should invest in improving the continent's digital infrastructure to support cross-border data flows. Stable and secure internet connections, along with data centres that meet global standards, are critical for enabling efficient data transfer. This investment is particularly crucial in the context of emerging technologies such as artificial intelligence and the Internet of Things, which rely heavily on real-time data access and processing. Governments can incentivize private sector investments in digital infrastructure by offering tax breaks or public-private partnership opportunities.

15.4 Promote Public Awareness and Capacity Building

Businesses, especially small and medium-sized enterprises (SMEs), often lack the resources and knowledge to navigate complex data protection laws. Policymakers should launch initiatives aimed at educating businesses and the public about data protection best practices. This could include workshops, online resources, and partnerships with academic institutions to build local expertise in data governance. Capacity building is also essential for ensuring that local businesses can compete in a data-driven global economy, reducing the digital divide that currently hampers economic growth in many African countries.

15.5 Establish Clear Guidelines for Data Transfers

Businesses require clear and practical guidelines to manage data transfers across borders. Policymakers should define the conditions under which data can be transferred, including the adequacy of protections in recipient countries and the obligations of data controllers. Additionally, establishing regional guidelines for data transfer would help reduce the inconsistencies that currently exist across national frameworks. This would provide businesses with the clarity needed to engage confidently in cross-border trade, knowing they are in compliance with all relevant regulations.

16.0 Conclusion

In conclusion, cross-border data flows represent a critical component of Africa's integration into the global digital economy. This report has explored the legal frameworks, challenges, and opportunities associated with managing these flows, highlighting the importance of harmonising data protection laws across the continent. With digital trade becoming increasingly central to economic development, African nations must address the regulatory fragmentation that hinders efficient data transfers and limits their potential benefits. By investing in digital infrastructure, promoting regional cooperation, and ensuring robust data protection mechanisms, African countries can create a secure environment for data flows while safeguarding individual rights and fostering economic growth. The collaboration between governments, businesses, and regional bodies will be essential in building a resilient digital economy that maximises the benefits of cross-border data transfers for all stakeholders.

This study was made possible by a grant provided by the Hewlett Foundation.
We thank the organization for their continued support.

Strathmore University

Centre for Intellectual Property and Information Technology Law

Location: Ole Sangale Rd, Madaraka Estate.
Postal Address: P.O Box 59857-00200, Nairobi, Kenya.
Tel: +254 (0)703 034612
Email: cipit@strathmore.edu
Website: www.cipit.strathmore.edu