African Journal on Privacy & Data Protection

To cite: J Wanjiku & T Khaoma 'A case for continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa' (2024) 1
African Journal on Privacy & Data Protection 18-49

A case for continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa

*Joy Wanjiku**
Advocate of the High Court of Kenya

*Taria Khaoma***
Advocate of the High Court of Kenya

Abstract:

The widely cited analogy "data is the new asset" or "data is the new commodity" underscores the fundamental role of personal data in today's economic context. This was observed in the increase in the uptake of digital technologies and solutions that relied heavily on personal data following the COVID-19 pandemic. We live in a world where an individual's data collection takes place in one jurisdiction, and is processed and retained in another jurisdiction. Transferring personal data across international borders is a crucial element of the digital economy. Despite the benefits that would accrue to national economies and businesses by allowing data flows in the African region, African countries either do not have regulations

* Bachelor of Laws, Strathmore University and an Advocate of the High Court of Kenya. Commercial, Employment and IPT Associate at DLA Piper Africa, Kenya (IKM Advocates).
** Bachelor of Laws, Strathmore University. Advocate of the High Court of Kenya and member of the International Association of Privacy Professionals (IAPP). IP and TMT Associate at Bowmans Kenya (Coulson Harney LLP).

in place to address cross-border data transfers or have taken different approaches to regulation. Certain nations mandate that foreign countries adhere to specific minimum data privacy standards before allowing the transfer of data across their respective borders. The common standard of cross-border data transfers has been an adequate level of data protection by the recipient country, but what is an adequate level of data protection? The unforeseen result of these fragmented measures is the localisation of data, primarily because of the variations in how countries safeguard data, or the recipient's incapacity to guarantee the sender that they will adequately protect the data of their citizens.

Key words: data localisation; African Union; cross-border data transfer; adequacy decisions; data protection

1 Introduction

For centuries information has been circulating worldwide, and the means of transmission have evolved with time from international mail to transatlantic cables, subsequently to telephone cables. As digital transformation continues to spread across nations and industries, data flows are expected to surge even more.[1] In the modern data-driven world, cross-border data transfers have become an essential part of the global economy. The movement, storage and processing of data across borders serve as a foundational pillar for contemporary international trade and investments. This critical infrastructure bolsters the swift expansion of digital services and enterprises across the world.

In the throes of the COVID-19 pandemic, from 2020 to 2021, the global community depended heavily on international data transfers to synchronise economic operations both domestically and globally, alleviate the negative impacts on trade, and sustain essential value networks.[2] The occurrence of such events has underscored the pivotal role of cross-border data sharing in ensuring the continuity of a free market, where willing sellers and willing buyers can efficiently engage in commerce, making informed decisions, and facilitating global economic interactions. However, with the increase in data flows, concerns around data privacy, security, and protection have arisen, leading to various regulatory approaches across different regions.

Cross-border data flows encompass the transfer and movement of data or information between servers across the borders of distinct sovereign entities

1 N Cory & L Dascoli 'How barriers to cross-border data flows are spreading globally, what they cost, and how to address them' Information Technology and Innovation Foundation (2021), https://d1bcsfjk95uj19.cloudfront.net/sites/default/files/2021-data-localization.pdf (accessed 13 March 2023).

2 F Cilauro, S Snelson & A Breckenridge 'The economic impact of cross-border data flows' 17 June 2021, https://www.frontier-economics.com/uk/en/news-and-articles/news/news-article-i8493-the-economic-impact-of-cross-border-data-flows/# (accessed 23 September 2023).

using network equipment designed for such transmission.[3] These data flows empower individuals to convey information for online communication, monitor international supply chains, exchange research, offer services across borders, and foster technological advancements. The necessity of cross-border data transfers can vary depending on the agreements among data processors, controllers, owners, recipients, and the specific objectives behind such data transfers.[4]

In Africa there has been a significant shift in the realm of personal data protection following the introduction of the General Data Protection Regulations by the European Union (EU). This shift has spurred the adoption of local and regional regulations on data privacy across Africa, including the ECOWAS Data Protection Act in 2010, the East Africa Community Legal Framework for Cyber Laws in 2010, and the Southern African Development Community Model on Electronic Transactions and Electronic Commerce.[5]

Considering the afore-mentioned, cross-border data transfers have become a complex issue due to the different approaches to data protection, leading to disjointed measures and unintended consequences, such as data localisation. Presently, African governments are leaning on their own national data protection regulations, and cross-border data transfers are particularly allowed contingent upon the existence of appropriate safeguards and data protection regulations in the recipient state that ensure the protection of personal data. Furthermore, the level of control over cross-border data transfers within free trade agreements (FTAs) and preferential trade agreements (PTAs) in Africa varies widely. Some of the current provisions pertain to data protection in cross-border transfers, whereas others make no reference to this aspect at all.[6]

The absence of a harmonised framework on cross-border data transfers has hindered the free flow of data in Africa, resulting in negative consequences for businesses and the economy at large. When there is a legislative gap, the personal data of consumers, who are the data subjects, becomes vulnerable to potential compromise and attacks from cybercriminals, identity theft, unauthorised access by foreign surveillance and law enforcement agencies, and other risks. These individuals may not receive the necessary recourse or protection.[7] Therefore, for a region that has no model to govern the free flow of data across borders, there is a dire need for continental cooperation and development of a regional legal framework to govern cross-border data transfers, given the potential benefits to

3 Congressional Research Service 'Data flows, online privacy, and trade policy' (2020) https://sgp.fas.org/crs/misc/R45584.pdf (accessed 23 September 2023).
4 N Rotich 'Examining cross-border data flows provisions in Africa's free trade agreements' 31 August 2023, https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/ (accessed 23 September 2023).
5 C Ewulum 'The legal regime for cross-border data transfer in Africa: A critical analysis' LLB dissertation, University of Nigeria, 2023 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4546964 (accessed 23 September 2023).
6 Rotich (n 4).
7 Ewulum (n 5) 5.

national economies and businesses. As per the United Nations (UN) Conference on Trade and Development (UNCTAD), 'effective data protection is closely intertwined with digital trade in goods and services, as inadequate safeguards can erode consumer confidence, leading to adverse market consequences'.[8]

This article underscores the significance of cross-border data transfers, emphasising its abundance, while also considering the obstacles to such transfers, with a specific focus on data localisation. Additionally, the authors highlight how the absence of a unified legal framework for cross-border data flows has hindered the realisation of digital economy advantages. Consequently, the article contends that the African Union (AU) should assume a leading role in establishing a continental legal framework that strikes a balance between data protection and privacy concerns and the advantages of a fluid digital economy. By addressing the present state of cross-border data transfers in Africa and advocating a cohesive legal framework, the article aims to foster continental collaboration, ultimately benefiting national economies and businesses.

2 The roadmap of cross-border data transfers

The growing importance of data in today's digital economy has led to a significant increase in cross-border data transfers. However, this process is not without its challenges. Various legal, technical, and cultural barriers can impede the smooth flow of data across borders. This roadmap of cross-border data transfers draws attention to the series of steps that need to be taken to ensure the safe and secure transfer of data between countries. It begins with the creation and implementation of strong data protection legislation, which includes data security requirements for both public and private sector organisations; the issuance of consent where necessary; ensuring that safeguarding measures are in place for both parties; and receipt of the data.

To facilitate cross-border data transfers, policy makers and industry leaders have developed a roadmap that outlines the key steps necessary for the seamless and secure movement of data between countries. This roadmap includes measures such as binding corporate rules, standard contracts, adequacy decisions, data localisation requirements, data security regulations, and cross-border data transfer agreements. In this part we explore the roadmap of cross-border data transfers and examine the various steps involved in ensuring that data is transferred safely and efficiently across borders.

8 As above.

2.1 Why must data be moved across borders?

Data lacks the attributes of scarcity typically associated with tangible goods or services, as it possesses the inherent qualities of shareability, reusability, and non-depletion.[9] The cross-border transfer of data is a critical component of the digital economy, enabling businesses to operate across borders, facilitating global collaboration, and supporting the adoption of digital technologies. As technological transformation progresses, the collection and processing of data is accelerating through machine-learning products and services such as artificial intelligence and internet of things that are increasingly able to produce, store and analyse an unprecedented amount of data without human intervention.[10] Global data flows are a consequence of the increasing trends of globalisation and digitalisation in business and society, forming a vital foundation for the modern economy. The ability to utilise, share and access information across international boundaries not only stimulates creativity but also empowers the creation of data-driven products and services, driving economic growth and nurturing the generation of new concepts. Furthermore, it often serves as an essential resource for remote communities.[11]

The African Continental Free Trade Agreement (AfCFTA) is centred around economic integration and the promotion of trade whilst carrying significant data protection considerations. One of its primary objectives is the creation of a single market for goods, services, facilitated by movement of persons in order to deepen the economic integration in Africa.[12] AfCFTA aims to enable the unrestricted movement of goods, services and individuals across African borders, inevitably leading to the exchange of data as businesses partake in cross-border transactions. In order to ensure the seamless functioning of AfCFTA, it becomes essential to establish a unified data protection framework for effectively managing cross-border data flows while upholding data privacy laws and regulations. While recognising the state parties' authority to regulate their territories and pursue legitimate policy goals, AfCFTA is also mindful of the importance of creating explicit, transparent, predictable, and mutually beneficial regulations to govern trade in goods and services, competition policy, and intellectual property investment.[13]

Moreover, from a cybersecurity perspective, some states may believe that data is more secure when it is stored within its national borders. However, cross-border data transfers are critical to cybersecurity partly because they allow for

9 United Nations Development Programme 'Enabling cross-border data flow in ASEAN and beyond' (2021), Enabling-cross-border-data-flow-asean-and-beyond-report.pdf (accessed 23 September 2023).
10 As above.
11 Centre for Information Policy Leadership 'Cross-border transfer mechanisms' (2015), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf (accessed 23 September 2023).
12 African Continental Free Trade Agreement 2018 art 3(a).
13 Ewulum (n 5) 28.

cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data.[14] Storing all data in one geographical territory, contrary to allowing cross-border data flows, reduces risk detection, assessment and response to cyberthreats in a particular country.[15] When governments mandate localisation or restrict the ability to transfer and analyse the free flow of data, the onus of maintaining the security of data becomes a core function of the data controller or data processor. Security is determined by the technical, administrative and operational protections, put in place by the service provider, that accompany the data, not the location.[16] Therefore, regardless of whether or not governments impose data localisation requirements, it might not necessarily mitigate a security breach.

By limiting the flow of data across borders, the process of detecting suspicious activities becomes more complex. Criminals can exploit gaps in cross-border data sharing to commit crimes such as fraud, money laundering and terrorism financing. 'A criminal rejected in one country can open a mobile money account and make transactions in another country.'[17] In order to ensure a robust national security system across a geographically dispersed network, policy makers need to avoid misguided frameworks that limit the default flow of data. However, it is also important to strike a balance between cross-border data sharing and data protection. While an open and unrestricted flow of data can facilitate crime detection and prevention, it can also compromise data security and privacy. In addition, localising data in one system may lead to lower investment in security and create vulnerabilities that can be exploited by cybercriminals.

2.2 The pathway for moving data across borders

To facilitate the safe and secure transfer of data, several conditions must be fulfilled. These conditions encompass setting a baseline level of data protection; giving cybersecurity a high priority; binding corporate rules; the presence of adequacy decisions and consent from data subjects ensuring hardware accountability across nations; as well as prioritising technical interoperability, data portability and data provenance. Furthermore, it is crucial to ensure that the policy environment is future-proof, so it remains effective and relevant as technology evolves.

14 Global Data Alliance 'Cross-border data transfers and cybersecurity', https://globaldataalliance.org/issues/cybersecurity/ (accessed 30 March 2023).

15 World Economic Forum 'A roadmap for cross-border data flows' (2020), https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf (accessed 23 September 2023).

16 Cory & Dascoli (n 1) 13.

17 C Scharwatt 'The impact of data localisation requirements on the growth of mobile money-enabled remittance GSMA' (2019), https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf (accessed 23 September 2023).

2.2.1 Establishing an adequate level of data protection

Cross-border transfers of data should generally be permitted under national legislation to enhance trust and allow for regulatory compliance across borders. Almost 72 per cent of countries have full or draft legislation on data protection and privacy. To date, 36 out of 54 African countries have data protection laws and regulations, with 16 countries having signed the Malabo Convention and 13 countries having ratified it.[18] As expected, these laws governing the collection, processing and transfer of data, be it personal identifiable information or sensitive personal identifiable information, vary from country to country.[19] Despite the diverging data protection regulations, there are core principles of data protection that remain fairly consistent from jurisdiction to jurisdiction. These principles include fair and lawful processing of data; purpose specification; minimality; quality; transparency; data subject participation; sensitivity; confidentiality; and accountability. Any differences that may appear are significant to whether a particular data protection law will be a hard or a soft barrier to cross-border data transfer.[20]

When establishing an adequate level of data protection, UNCTAD states that when it comes to cross-border data transfers, countries have either one-off or ongoing exceptions.[21] In one-off exceptions, including allowing the data transfer based on performance of a contract between the data subject and the data controller or the data controller and the data subject, the transfer is based on the exercising of a legal right, and the transfer is necessary in order to protect the vital interests of the data subject. On the other hand, ongoing exceptions include the adequacy approach, where a regulator in a particular jurisdiction issues a whitelist of countries with a sufficient degree of protection that allows for the transfer of personal data. The issuance of white-list countries with sufficient data protection laws has been seen in the EU.

Second, another ongoing exemption approach is the implementation of binding corporate rules by multinational companies. These rules are established as enforceable internal guidelines for handling cross-border data transfers within the company group. This enables multinational corporations to share personal

18 A Sylla 'Recent developments in African data protections laws' 24 February 2023, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2023 (accessed 18 March 2023).

19 General Data Protection Regulation (EU) 2016/679 of 2016 sec 4. 'Personal identifiable information' means any information relating to an identified or identifiable natural person such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. 'Sensitive personal identifiable information' means all personal data including racial, political, religious, trade union membership, genetic, biometric, sexual orientation, and health details of individuals.

20 World Economic Forum (n 15) 22.

21 United Nations Conference on Trade and Development 'Data protection regulations and international data flows: Implications for trade and development' (2016), https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed 25 September 2023).

data internationally among their group entities, even when the destination country lacks sufficient data protection measures.[22] The binding corporate rules approach differs from the standard clauses approach, which relies on specific contract language to ensure an adequate level of data protection during transfers. Standard contract clauses typically are effective for smaller companies and when data sharing occurs between only two parties.

Furthermore, in some jurisdictions consent has been used as the foundation for cross-border data transfers. This approach hinges on individuals willingly and explicitly providing their consent for their data to be transferred beyond a specific jurisdiction. However, in most cases, relying on consent for cross-border data transfers is subject to additional conditions and requirements.

Therefore, the question arises as to how we can facilitate cross-border data transfers whilst establishing an adequate level of data protection. Data privacy concerns can be addressed by governments through mandating contractual commitments that require parties to adhere to core privacy principles during transfer of data.[23] In this way, regulators are able to enforce partial restrictions that may be helpful to ensure sufficient levels of data protection abroad, they can also hold data transferring companies responsible for consequences caused and are able to apply and enforce national laws against foreign companies. The challenge around protective contracts is that if not harmonised regionally, every country then requires its own contract with its own clauses, causing an undue burden on international trade by requiring multi-nationals to constantly review and execute millions of contractual terms.

2.2.2 Prioritising cybersecurity and jurisdictional accountability

Cybersecurity involves taking steps to protect data from unauthorised access, commonly referred to as cyber attacks. These measures are designed to ensure that data being transferred is received only by its intended recipient and not intercepted or accessed by unauthorised parties.[24] Companies may choose to store data at geographically-diverse locations to obscure the location of data and reduce the risk of physical attacks. Additionally, this enables companies to reduce

22 Price Waterhouse Coopers 'Binding Corporate Rules. The General Data Protection Legislation' https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf (accessed 25 September 2023).

23 World Economic Forum (n 15) 23.

24 A Beyleveld & F Sucker 'Cross-border data flows in Africa: Policy Considerations for the African Continental Free Trade Area Protocol on Digital Trade' Centre for the Studies of Economies of Africa (2022), https://cseaafrica.org/wp-content/uploads/2022/10/2022-10-28-CSEA__MI__Report-on-Cross-Border-Data-Flows-in-Africa__Policy-Considerations-for-the-AfCFTA-Protocol-on-Digital-Trade.pdf (accessed 25 September 2023).

network latency, to maintain redundancy and resilience for critical data in the wake of physical damage to the storage location.[25]

To establish themselves as reliable recipients of cross-border data, nations must implement rigorous data security laws that mandate data protection standards for both public and private entities, alongside measures for reporting security breaches. Furthermore, governments should consider establishing mutual contractual obligations as a basis for mutual legal assistance and reciprocal transfers of law enforcement data, allowing for the lawful transfer of data. It is important for governments to avoid any attempts to gain unauthorised data access or implement technology backdoors throughout these processes.[26]

Cross-border data-sharing agreements between governments should include mandatory data security measures and an anti-snooping clause, which prohibits governments and connectivity providers from viewing transmitted data across borders except in certain prescribed instances.[27] Additionally, a clear cooperation mechanism between authorities should be established to enhance trust in the data transfer process. These measures may help promote a safe and secure environment for cross-border data transfer while protecting the privacy and security of individuals' data.

2.2.3 Prioritising technical interoperability, data portability and data provenance

Technical interoperability

Technical interoperability pertains to the capacity to exchange data among various systems and empower these systems to effectively utilise the shared data.[28] Technical interoperability can manifest in a syntactic form, necessitating the communication and data exchange among multiple systems, irrespective of variations in programming languages. Alternatively, it may take on a semantic nature, demanding that an individual system comprehends and facilitates the meaningful utilisation of shared data or resources by individuals, organisations and public services.[29]

25 Global Data Alliance 'Cross-border data transfers and data localisation' February 2020, https://globaldataalliance.org/wp-content/uploads/2021/07/02112020GDAcrossborderdata.pdf (accessed 3 March 2023).
26 Global Data Alliance (n 14).
27 World Economic Forum (n 15) 25.
28 A Mittal 'Catalogue of technical standards for digital identification systems' (2022), documents1.worldbank.org/curated/en/707151536126464867/pdf/Catalog-of-Technical-Standards-for-Digital-Identification-Systems.pdf (accessed 25 September 2023).
29 World Economic Forum (n 15) 33.

To ensure that information is accessible and usable in any jurisdiction, systems must possess data interoperability and interconnectivity. This enables data to move seamlessly in the required format to those who require it, when they require it.[30] Practically data is collected and retained by many organisations at global, national and local levels either in an unstructured or structured way. This type of storing and processing of data negates its difficulty to use the data cross-functionally with databases owned by other organisations.[31] Consequently, disseminating or exchanging data among different disconnected applications can pose challenges, given the absence of a standardised format or representation, which complicates its cross-industry utilisation in fields such as artificial intelligence and the internet of things. From our research, we have noted that this can impede cross-border data sharing as data will not be seamlessly transmitted across borders.

The complexity for companies aiming to achieve interoperability and interconnectivity in cross-border data is high, and before transferring data across borders, companies must –

- have a clear understanding of the data protection regulations that apply. This aids companies to understand their obligations under the applicable regime either as a data controller or a data processor.
- conduct a data-mapping exercise to identify and classify the data to be transferred amongst the data collected. Not all data is suitable for cross-border transfers, especially sensitive personal information.
- anonymise or pseudonymise data whenever possible to reduce privacy risks together with using strong encryption methods to protect data during transit and storage. This ensures that even if intercepted, the data remains unreadable to unauthorised parties.
- consider using mechanisms such as standard contractual clauses (SCCs), binding corporate rules (BCRs), or obtaining approval from relevant data protection authorities to legitimise cross-border data transfers.
- assess the necessity of data localisation mandates and the requirement to host data within designated geographic areas to ensure compliance with local data sovereignty regulations.
- enforce rigorous access restrictions and authentication systems to guarantee that only authorised individuals can access and move data; employ role-based access controls (RBAC) to restrict data access to individuals with relevant permissions.
- be transparent with data subjects about the cross-border data transfers, their purpose, and the measures in place to protect their data.
- maintain comprehensive audit trails to track data transfers and access; regularly monitor and review these logs to detect and respond to any unauthorised or suspicious activities.

To attain data interoperability and seamless integration as mentioned above, organisations must fully harness the potential of merging diverse datasets, whether employing fundamental algorithms or artificial intelligence techniques. As this information will be finally harmonised, standardised and stored in

30 United Nations Development Programme (n 11).
31 World Economic Forum (n 15) 35.

structured databases, it will promote data flows to those who need it, where they need it, when they need it, and in the form in which they need it.[32]

Data portability and data provenance

Data portability empowers individuals to move their data between different systems, granting them authority and ownership of their personal data. It also offers a means for users to transition between different service providers.[33] It also provides users with the flexibility to switch between service providers. This issue is particularly important for customers of software as a service (SaaS), who may face challenges when switching services due to data localisation restrictions, which could result in vendor dependency.[34] Vendor entrenchment occurs when pricing models, physical network infrastructure, or unfair contractual clauses create hurdles in transitioning away from a current system, thus obstructing data movement and acting as a barrier to new market entrants. Governments can foster data portability by discouraging vendor entrenchment practices and advocating interoperability standards.

In choosing the best approach to finding the solution to avoid vendor lock-ins, governments can consider either the open standards approach or the open source technologies approach. By adopting an open standards methodology, developers delineate the elements of a system and specify their interactions. This standardisation of system components and communication methods enhances the flexibility and neutrality of systems. In this approach, governments will face reduced risks of becoming bound by exclusive contracts since patents and other proprietary concerns no longer pose obstacles that enable access to raw data and portability. Conversely, the open-source approach involves customers diving into the source code of non-standard parts, rebuilding them, and creating standardised connections. This process may lead to effective solutions but may take years due to design, development and testing.[35]

The significance of data provenance lies in its ability to establish the source of data, its owner, the entities that have processed it, and its complete history from the point of collection, all of which are crucial for safeguarding data authenticity.[36] Blockchain technology has the potential to create a tamper-evident record of data, ensuring that every occurrence of data being transferred or subjected to any form of manipulation can be traced. However, it can prove to be difficult to ascertain the origins of de-identified data or data devoid of historical context. In

32 As above.
33 Organisation for Economic Cooperation and Development 'Mapping approaches to data and data flows report for the G20 Digital Economy Task Force' (2020), http://www.oecd.org/trade/documents/mapping-approaches-todata-and-data-flows.pdf (accessed 25 September 2023).
34 United Nations Development Programme (n 9).
35 ID4Africa ' Putting government back in control Solving vendor lock-in with open standards' 20 June 2019, id4africa.com/2019/almanac/SECURE-IDENTITY-ALLIANCE-SIA.pdf (accessed 20 September 2023).
36 World Economic Forum (n 15) 36.

instances such as these, designating the data as lacking provenance may assist users in evaluating potential risks to data quality when making decisions regarding its appropriate utilisation. Although data provenance is typically viewed as a technical concern, ensuring the accurate attribution of data's origins through proper implementation can elevate data quality during the sharing and transfer of data across geographical boundaries.[37]

2.2.4 Future proofing the policy environment

As the global digital economy continues to expand, the need for cross-border data transfers is becoming increasingly important. However, concerns about data privacy and security have prompted many governments to enact strict regulations around cross-border data sharing. To address these concerns and future proof the policy environment, policy makers must carefully consider the potential risks to and benefits of cross-border data transfers, and develop policies that balance the need for data sharing with the need for data security and privacy. This may include enacting strong data security legislation, implementing mandatory data security measures in cross-border data-sharing agreements, and establishing clear cooperation mechanisms between authorities. By taking a proactive approach to future proofing, the policy environment around cross-border data transfers, governments can help promote a safe and secure environment for data sharing while protecting the privacy and security of individuals' data.

3 Barrier to cross-border data transfers: A spotlight on data localisation

Data localisation pertains to the mandate that data originating from a country's citizens or residents must initially be gathered, handled or stored within the geographical confines of a specific jurisdiction, such as a nation or a regional economic community or union.[38] Some argue that it may be easier to persuade policy makers to recognise the drawbacks of data localisation requirements and convince them to repeal such regulations, rather than attempting to find a common ground for the various data localisation requirements imposed by different jurisdictions.[39] These regulations, despite their intentions to promote data security and privacy, often come with a double-edged sword for businesses. They impose a twofold set of requirements on data processing and storage,

37 F Casalini & J López González 'Trade and cross-border data flows' OECD Trade Policy Papers 220 (2019), https://doi.org/10.1787/18166873 (accessed 17 March 2023).

38 Collaboration on International ICT Policy for East and Southern Africa (CIPESA) "Which way for data localisation in Africa?' (2020), https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf (accessed 15 March 2023).

39 Hunton & Williams LLP and the United States Chamber of Commerce 'Business without borders: The importance of cross-border data transfers to global prosperity' (2014), https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf (accessed 15 March 2023).

leading to the inevitable incurrence of additional expenses that otherwise would be avoided if companies had access to the cost-effective and efficient data services hosted in the cloud or international data centres.

The initial form of data localisation arises when governments impose limitations on the cross-border transfer of specific data types. These include personal data; health data; government data; financial data encompassing banking; credit reports; taxation and insurance, along with data associated with user-generated content on internet service platforms; subscriber data; and data held by e-commerce operators. Nations are expanding data localisation requirements by implementing comprehensive regulations that vaguely define the categories of data considered 'sensitive', 'crucial', or pertinent to national security.[40] On the other hand, we have data localisation regulations that require data controllers and data processors to undertake data collection, processing and storage domestically.[41] This not only makes data transfers very complicated, costly and uncertain, but also creates a type of *de facto* localisation where companies have no other option but to store the data locally, especially in the face of massive fines.

Many countries are adopting data-localisation measures due to various reasons, one of which is the desire to exercise greater control over valuable digital assets. While this kind of digital protectionism is a key factor driving these measures, it has been overshadowed by the larger concept of cyber sovereignty, which encompasses the idea of exerting control over digital activities and assets. The significance of data has in recent years experienced a substantial rise, and countries may wish to have this asset closer to them for both psychological and practical reasons. However, simply having data stored locally is not sufficient to create value in and of itself.[42]

Additionally, it is important to highlight that, while data-localisation issues may not be tackled at the local or regional levels, they are, to some extent, being addressed, through international trade agreements such as the Trans-Pacific Partnership (TPP).[43] The TPP provides a test for imposition of data-localisation requirements by signatories with national laws that restrict cross-border transfers. It states that signatories that intend to restrict cross border data flows must satisfy the following:

(1) Is the law necessary to achieve a valid public policy goal?
(2) Is the law free from arbitrary or unjustifiable discrimination in its application?
(3) Does the law avoid being a hidden trade restriction?
(4) Does the law impose information transfer restrictions beyond what is needed to achieve its goal?

40 Cory & Dascoli (n 1) 15.
41 Scharwatt (n 17).
42 Collaboration on International ICT Policy for East and Southern Africa (n 38).
43 UNCTAD (n 21) 14.

The four-part test above may be used as a global test for determining whether data-localisation requirements are excessive.

Restricting data flows has a significant impact on a nation's economy as it measurably reduces the volume of trade, lowers its productivity and increases the prices for small and medium enterprises that are digitally focused and rely on data. Such businesses are an essential growth sector for any country. From a broader private sector perspective, data localisation disincentives the entry of international firms, leading to less competition but, then, foreign companies lack any incentive to invest as they foresee a future where they will incur additional capital and operational expenditure to create local data storage, data centres and other infrastructure.[44] While data-localisation practices are often viewed as a means of protecting citizens' personal data, they may not be effective without robust data protection legislation and a comprehensive approach to controlling data regardless of its physical location.[45] Therefore, we have to ask ourselves whether data localisation requirements are ever justified.

4 Current regulatory framework for cross-border data transfers in Africa

As the digital landscape continues to expand across the African continent, there has been an increasing need to regulate cross-border data transfers. In this part we explore the various regulatory initiatives taking place at the continental, regional and national levels, in a bid to create a robust and secure environment for cross-border data transfer.

4.1 Continental and regional frameworks

4.1.1 African Union

Article 14(6)(a) of the African Union Convention on Cyber Security and Personal Data Protection, 2014 provides that the data controller should not transfer personal data to a non-member state of the AU unless such a state ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data is being or is likely to be processed. The Convention, however, does not set out what would be considered an adequate level of protection or the factors to be taken into account when assessing the adequacy in the level of protection. Article 14(6)(b) adds that this prohibition is not applicable where

44 United Nations Development Programme (n 9).
45 World Economic Forum (n 15) 23.

the data controller requests authorisation for data transfer from the national data protection authority before transferring any personal data to the third country.[46]

As of 30 September 2023, only 15 countries had ratified the Convention. These are Angola, Cape Verde, Congo, Côte d'Ivoire, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo and Zambia.[47] The Convention entered into force 30 days after the 15th instrument of ratification had been deposited with the Chairperson of the AU, that is, on 8 June 2023.[48] While a number of countries covered in 4.2 below have data protection laws, most of them are yet to ratify the Convention. This highlights the need for increased efforts to promote and implement the Convention's provisions across the continent. Further, despite the developments across the world in relation to the transfer of personal data, the Convention has not been amended since it was drafted. There is a need for the AU to consider amendments to the Convention as a step towards the harmonisation of standards for the transfer of personal data across the continent.

Section 5.4.5 of the AU Data Policy Framework, 2022 sets out the following recommendations for cross-border data flows, among others: Data-protection frameworks ought to provide minimum standards for cross-border data transfers; the establishment of norms and standards should expressly ensure reciprocity as a central principle for permitting cross-border flows; a degree of capacity must be provided across data-protection agencies to ensure effective cross-border resolution; and AU member states should define a framework and modalities to regulate cross-border data transfers and identify the African entity and persons entitled to manage this system.[49]

Section 5.5.3 of the Framework lists proposed actions in relation to continental instruments. These include that member states should ratify the Malabo Convention and develop additional protocols; to reflect changes since the drafting of the Convention; and to agree on common and harmonious criteria for assessing adequacy in the levels of protection of personal data across the continent to facilitate and enable cross-border transfer of data and to standardise protection.[50]

The digital transformation strategy for Africa highlights policy recommendations and proposed actions. These include support interventions to strengthen cybersecurity at national level such as accelerating the establishment

46 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) art 14.
47 African Union, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf (accessed 31 March 2023).
48 Malabo Convention (n 46) art 36.
49 African Union, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf (accessed 31 March 2023).
50 As above.

of personal data protection authorities and making the Malabo Convention consistent with standards such as the modernised Convention 108, the General Data Protection Regulation (GDPR) to promote competitiveness of African companies outside the continent. Support interventions to strengthen cybersecurity at regional and continental level include establishing a framework and mechanism for regional cooperation and mutual assistance and strengthening cooperation between AU bodies and the authorities for the protection of personal data.[51]

4.1.2 Southern African Development Community

The SADC Model Law, 2013 sets out requirements for the transfer of personal data to: a member state that has incorporated the model law into its national laws; a member state that has not incorporated the Model Law into its national laws and to a non-member state. The Model Law permits the transfer of personal data to recipients subject to national law that has been adopted for implementation of the Model Law if the recipient establishes that the transfer of personal data is necessary for the performance of a task carried out in the public interest or subject to the exercise of public body, or if the recipient establishes that it is necessary to transfer the personal data and there is no reason to presume that the data subject's legitimate interests would be prejudiced.[52]

The Model Law also permits the transfer of personal data to recipients other than member states of the SADC that have not incorporated the Model Law Into their national laws on the basis of an adequate level of protection being ensured in the recipient's country, unambiguous consent of the data subject or necessity.[53] The adequacy of the level of protection afforded by the third country shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations. The factors that shall be considered include the nature of the data; the purpose and duration of the proposed processing operation(s); the recipient third country; the laws in force in the third country in question and the professional rules and security measures that are complied with in that third country.[54] The transfer of personal data is also permitted where the transfer is made from a register that is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled.[55]

Out of the 16 member states, only five countries, Angola, Mozambique, Mauritius, Namibia and Zambia, have ratified the Malabo Convention. Eleven

51 Digital Transformation Strategy for Africa (2020-2030).
52 Southern African Development Community Model Law (Model Law) 2013 art 43.
53 Model Law arts 44 & 45.
54 Model Law art 44(1)(b).
55 Model Law art 45(1)(f).

countries, Angola, Botswana, Eswatini, Lesotho, Madagascar, Mauritius, Seychelles, South Africa, Tanzania, Zambia and Zimbabwe have enacted data-protection laws. Three countries, Angola, Mauritius and South Africa, have established a data-protection authority.

4.1.3 Economic Community of West African States

Article 36 of the Supplementary Act on Personal Data Protection within the ECOWAS Act, 2010 provides that a data controller shall transfer personal data to a non-member of an ECOWAS country where the country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data. The Act, however, does not set out what would be considered an adequate level of protection or the factors to be taken into account when assessing the adequacy in the level of protection. The data controller is required to inform the data protection authority before transferring personal data to a third country.[56]

Out of the 15 member states, only seven countries, namely, Cape Verde, Côte d'Ivoire, Ghana, Guinea, Niger, Senegal and Togo, have ratified the Malabo Convention. Ten countries, Benin, Cape Verde, Côte d'Ivoire, Ghana, Guinea, Mali, Niger, Nigeria, Senegal and Togo, have enacted data-protection laws. Eight countries, Benin, Cape Verde, Côte d'Ivoire, Ghana, Mali, Niger, Nigeria and Senegal, have established a data-protection authority.

4.1.4 East African Community

Recommendation 19 of the Draft EAC Legal Framework for Cyber Laws recommends that further work needs to carried out on the issue of data protection and privacy, to ensure that the privacy of citizens is not eroded through the internet, that legislation providing for access to official information is appropriately taken into account, the institutional implications of such reforms and to take into account fully international best practice in the area.[57]

Out of the seven member states, only Rwanda has ratified the Malabo Convention. Four countries, Kenya, Rwanda, Tanzania and Uganda, have enacted data-protection laws. Three countries, Kenya, Rwanda and Uganda, have established a data-protection authority.

Despite the regional focus of many cross-border data transfer regulations in Africa, the efficacy of such frameworks often hinges on the adequacy of data protection measures in the recipient country, regardless of whether it is a member state of that regional organisation. In practice, this means that countries

56 Supplementary Act on Personal Data Protection within ECOWAS Act, 2010 art 36.
57 Draft EAC Legal Framework for Cyber Laws, 2008.

with robust data-protection safeguards can often bypass regional regulations and facilitate cross-border data transfers more freely than their counterparts without such protections.

4.2 National frameworks

While there are 36 African countries that have enacted data protection laws, we have restricted our review to 17 countries that have official versions of their legislation available in English. Other than the countries highlighted below, Algeria, Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Egypt, Gabon, Guinea, Madagascar, Mali, Mauritania, Morocco, Niger, Republic of Congo, Senegal, Somalia, Togo and Tunisia, have data-protection laws in place.

4.2.1 Botswana

Section 48 of the Data Protection Act prohibits the transfer of personal data to another country. The Act allows the Minister to designate the transfer of personal data to any country listed in the Order.[58] In 2022 the Minister for State President issued the Transfer of Personal Data Order, pursuant to section 48(2) of the Act, declaring that personal data may be transferred to the 45 countries listed in the order.[59] It is notable that there are only two African countries, South Africa and Kenya; that are included in the Order. The criteria used to determine the countries, however, is unclear.

Despite the restriction in section 48 of the Act, section 49 allows the transfer of personal data on similar bases to those covered in articles 44 and 45 of the SADC Model Law.

4.2.2 Cape Verde

Article 19 of the Data Protection Act provides that the transfer of personal data that are undergoing processing or intended for processing may only take place subject to compliance with the Act and other legislation applicable to issues of personal data protection, and undergoing processing for transfer to another country that has an adequate level of data protection.[60] This adequate level of protection should be assessed in light of all the circumstances surrounding a data transfer or a set of data transfers, in particular, the nature of the data; the purpose and duration of the proposed processing; the country of origin and country of final destination; the rules of law in force in the state in question; and the professional rules and security measures that are complied with in that country.[61]

58 Data Protection Act 32 of 2018 sec 48.
59 Transfer of Personal Data Order, 2022.
60 Data Protection Act Law 133/V/2001 of 22 January (Law 133/V/2001) art 19(2).
61 Law 133/V/2001 (n 60) art 19(3).

The Act permits the transfer of personal data to third countries that do not ensure adequate security safeguards on the basis of unequivocal consent of the data subject, necessity or where the transfer is made from a public register that is intended for information of the public and which is open to consultation either by the general public or by any person who can demonstrate legitimate interest.[62] It is interesting to note that despite the fact that Cape Verde is not an SADC member state, the provisions on transfer of personal data are similar to those covered in articles 44 and 45 of the SADC Model Law.

4.2.3 Côte d'Ivoire

Law 2013-450 provides that a person responsible for the processing can be allowed to transfer personal data to a third country only if the state provides a higher level of protection or equivalent privacy, freedoms and fundamental rights of individuals with regard to the processing which the data are or may be subjected. The person is also required to obtain permission from the protection body before any transfer of personal data.[63] These provisions are similar to those in the Supplementary Act on Personal Data Protection within ECOWAS Act, 2010.

4.2.4 Eswatini

The provisions on cross-border transfer of personal data outside Eswatini under the Data Protection Act are similar to articles 43, 44 and 45 of the SADC Model Law.[64] The Act provides for transfer of personal information within SADC and non-SADC member states.

4.2.5 Ghana

While Ghana has a data protection law, the Data Protection Act contains no provisions on cross-border transfer of personal data.

4.2.6 Kenya

The Data Protection (General) Regulations require a data controller or data processor who is transferring personal data to a country outside Kenya to ascertain that the transfer is based on appropriate data protection safeguards, an adequacy decision made by the data commissioner, necessity or consent of the data subject.[65] A transfer of personal data is based on the existence of appropriate

62 Law 133/V/2001 (n 60) art 20.
63 Law 2013-450 dated June 19 2013 art 26.
64 Data Protection Act 5 of 2022 secs 32 & 33.
65 Data Protection (General) Regulations 2021 (General Regulations) reg 40.

safeguards where a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations or the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.[66]

A country is also deemed to have appropriate safeguards if it has ratified the Malabo Convention, a reciprocal data protection agreement with Kenya or a contractual binding corporate rules among a concerned group of undertakings or enterprises.[67] The first basis currently is questionable as Kenya is yet to sign and ratify the Malabo Convention.

4.2.7 Lesotho

The Data Protection Act imposes limitations on the transfer of personal data to a foreign third party. The recipient must be subject to a law, code of conduct or contract that effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles under the Act, and includes provisions that are substantially similar to those relating to further transfer of personal information from the recipient to third parties in foreign countries.[68] The Act also permits the transfer of personal data on the basis of consent of the data subject or necessity.[69] The Act also has a very unique basis for transfer, where the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer or, if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.[70]

4.2.8 Mauritius

The Data Protection Act allows a data controller or data processor to transfer personal data to another country on the basis of providing to the commissioner proof of appropriate safeguards, the data subject's explicit consent to the proposed transfer, necessity or the transfer being made from a register that, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest.[71]

66 General Regulations (n 65) reg 41(1).
67 General Regulations (n 65) reg 42.
68 Data Protection Act 5 of 2011 sec 52.
69 As above.
70 As above.
71 Data Protection Act 20/2017 sec 36.

4.2.9 Nigeria

The Nigeria Data Protection Regulation permits the transfer of personal data to a foreign country or an international organisation where the National Information Technology Development Agency has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organisation in question ensures an adequate level of protection.[72] The Attorney-General of the Federation (HAGF) is required to take into consideration the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including public security, defence, national security and criminal law and the access of public authorities to personal data.[73]

Where the National Information Technology Development Agency or the HAGF has not issued a decision as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of personal data to a foreign country or an international organisation shall take place on one of the bases specified in the Regulation, that is, explicit consent of the data subject or necessity.[74] Nigeria recently enacted the Data Protection Act that contains additional provisions on transfer of personal data. The bases provided in the Act are similar to those in GDPR which are covered in part 5 below, that is, the recipient is subject to law on personal data, there are binding corporate rulers, contractual clauses, code of conduct or a certification mechanism that provides an adequate level of data protection that is similar to the Act.

4.2.10 Rwanda

The transfer of personal data to a third party outside Rwanda is permitted under the law relating to the Protection of Personal and Privacy if a data controller or data processor has obtained authorisation from the supervisory authority after providing proof of appropriate safeguards with respect to the protection of personal data, on the basis of consent of the data subject or necessity.[75]

4.2.11 São Tomé and Príncipe

Article 19 of the Law on Protection of Personal Data provides that the transfer of personal data to a place outside the national territory may only be carried out in compliance with the provisions of this law and if the legal order to which they are transferred ensures a suitable level of protection.[76] This adequate level of

72 Nigeria Data Protection Regulation 2019 (NDPR) part 2.11.
73 As above.
74 NDPR (n 72) part 2.12.
75 Law 058/2021 of 13 October 2021 relating to the protection of personal data and privacy art 48.
76 Law 03/2016 Protection of Personal Data (Law 03/2016) art 19(1).

protection should be assessed in light of all the circumstances surrounding a data transfer or a set of data transfers, taking into account, in particular, the nature of the data, the purpose and the duration of the processing or planned treatments, the countries of origin and of final destination, the general or special rules of law in force in the legal system concerned, as well as the professional rules and security measures that are respected in that same order.[77]

The Law also permits the transfer of personal data to third countries that do not ensure an adequate level of protection on the basis of unequivocal consent of the data subject, necessity or where the transfer is carried out on the basis of a public register that, according to the law or administrative regulation, is intended to inform the public and is open to consultation with the general public or any person who can prove a legitimate interest.[78]

4.2.12 Seychelles

The Data Protection Act takes a unique approach to the issue of the transfer of personal data where, instead of providing the grounds on which transfers would be permissible, it provides for a transfer prohibition notice. The Act provides that if it appears to the commissioner that a person registered as a data user or as a data user who also carries on a computer bureau proposes to transfer personal data held by him to a place outside the Seychelles, the commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question.[79]

The Act, however, is yet to come into operation, and on 16 March 2023 the Data Protection Bill which seeks to repeal the Act was published. The Bill has taken a unique approach by providing for conditions in which sensitive personal data may be transferred outside Seychelles. For transfer of personal data, this is subject to the recipient country being part of a cross-border privacy rules system that ensures that the system's standards are enforceable against the data controllers and data processors as part of the certification system and data controllers and data processors have implemented security measures using a risk-based approach.[80] This is a different approach to that taken by other African states given that there currently is no certification system in place and there is no reference made to recipient countries having an adequate level of data protection.

77 Law 03/2016 (n 76) art 19(2).
78 Law 03/2016 (n 76) art 20.
79 Data Protection Act 9 of 2003 sec 16.
80 Data Protection Bill 2023 clause 48(3).

4.2.13 South Africa

The Protection of Personal Information Act (POPIA) restricts the transfer of personal data to a third party who is in a foreign country unless the recipient of the information is subject to a law, binding corporate rules or binding agreement. The requirements should provide an adequate level of protection that effectively upholds the principles for reasonable processing of the information that are substantially similar to the information protection principles under the Act, and includes provisions that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person and includes provisions substantially similar to the provision relating to the further transfer of personal information from the recipient to third parties who are in a foreign country. [81]

The Act also permits the transfer of personal data on the basis of consent of the data subject or necessity.[82] The Act, similar to the Lesotho Data Protection Act, permits a data controller or data processor to transfer personal data, where the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer and, if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.[83]

4.2.14 Tanzania

The provisions on cross-border transfer of personal data outside Tanzania under the Personal Data Protection Act are similar to articles 43, 44 and 45 of the SADC Model Law. The Act provides for the transfer of personal data to states with and without a legal framework providing for adequate data protection. Tanzania also passed the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 that provide for the procedure and requirements for applications for transfer of personal data.

4.2.15 Uganda

The Data Protection and Privacy Act provides that where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that the country in which the data is processed or stored has adequate measures in place for the protection of personal data at the least equivalent to the protection provided by this Act or the data subject has consented.[84]

81 Protection of Personal Information Act 4 of 2013 sec 72.
82 As above.
83 As above.
84 Data Protection and Privacy Act 9 of 2019 sec 19.

The Data Protection and Privacy Regulations expound on this provision, highlighting that the data controller or data processor is required to provide proof of the adequate measures or the data subject's consent to the Personal Data Protection Office.[85] For purposes of transfer on the basis of the existence of adequate measures for protection of personal data, the office is required to publish a notice in the *Gazette* specifying the countries that have adequate measures in place for the protection of the personal data at least equivalent to the protection required by the Act.[86] It is only where a country does not appear on the list that the data controller or data processor will be required that the country has adequate measures in place.[87]

4.2.16 Zambia

The Data Protection Act provides that a data controller shall process and store personal data on a server or data centre located in Zambia. The Minister, however, may prescribe categories of personal data that may be stored outside Zambia.[88] Personal data other than data that is categorised in accordance with the above provision may be transferred outside the country where the data subject has consented, and the transfer is made subject to standard contracts or intra group schemes that have been approved by the Data Protection Commissioner; or the Minister, has prescribed that transfer outside the country is permissible; or the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.[89]

4.2.17 Zimbabwe

The Data Protection Act allows the transfer of personal data only where the country of the recipient ensures an adequate level of protection and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out.[90]

The adequacy of the level of protection afforded by the third country shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country, the laws relating to data protection in force in the third country in question and the professional rules and security measures that are complied with in that third country.[91]

85 Data Protection and Privacy Regulations 2021 reg 30(1).
86 Data Protection and Privacy Regulations (n 85) reg 30(4),
87 Data Protection and Privacy Regulations (n 85) reg 30(5).
88 Data Protection Act 3 of 2021 sec 70.
89 Data Protection Act (n 88) sec 71.
90 Data Protection Act 5/2021 sec 28.
91 As above.

The Act permits the transfer of personal data to third countries that do not ensure an adequate level of protection on the basis of unambiguous consent of the data subject, necessity or where the transfer is made from a public register that, according to acts or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.[92]

From the above review of the legislative frameworks in place in various African countries, it is clear that there are varied approaches to cross-border transfer. Most countries have taken the approach of adopting the provisions in regional instruments in the regional organisations of which they are members. The basis that is captured in most legal instruments is countries having in place an adequate level of protection to personal data. However, there are some countries that do not provide the factors to be considered in determining this and whether the data protection authorities will issue adequacy decisions to ensure that the data controllers and data processors are not required to assess the level of adequacy. Further, while having data protection laws in place is a step in the right direction, it is possible for the varying conditions to be considered as less of an aid and more of a limitation to cross-border transfer of personal data.

5 Approaches taken by other regions in regulation of cross-border data transfers

We now review approaches taken by other regions in the regulation of cross-border data transfers, with a focus on the European Union (EU) and the Asia-Pacific Economic Cooperation (APEC).

5.1 European Union

Chapter V of the EU General Data Protection Regulation (GDPR) provides for transfers of personal data to third countries or international organisations. The general principle for transfers is that any transfer of personal data that is undergoing or is intended for processing after transfer to a third country or an international organisation shall take place only if, subject to the other provisions of GDPR, the conditions laid down in chapter V are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.[93]

GDPR sets out two general bases for the transfer of personal data, namely, an adequacy decision or appropriate safeguards. A transfer of personal data to a third

92 Data Protection Act (n 90) sec 29.
93 General Data Protection Regulations 2016/679 (GDPR) art 44.

country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.[94] The Commission so far has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the UK GDPR and the Law Enforcement Directive, and Uruguay as providing adequate protection.[95]

GDPR also permits, in the absence of an adequacy decision, the transfers of personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[96] There are two categories of transfers subject to appropriate safeguards, namely, (i) appropriate safeguards without authorisation from a supervisory authority; and (ii) appropriate safeguards with authorisation from a supervisory authority.

The appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by a legally-binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the Commission; standard data protection clauses adopted by a supervisory authority and approved by the Commission; an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.[97]

Where authorisation from a supervisory authority is required for the transfer of personal data, the appropriate safeguards may be provided for in contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation or provisions that are inserted into administrative arrangements between public authorities or bodies, including enforceable and effective data subject rights.[98]

GDPR also provides that in the absence of an adequacy decision or appropriate safeguards, personal data may be transferred to a third country or international

94 GDPR (n 93) art 45.
95 European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 31 March 2023).
96 GDPR (n 93) art 46.
97 As above.
98 As above.

organisation on the basis of a data subject's explicit consent, necessity or where the transfer is made from a register which according to EU or member state law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can prove a legitimate interest.[99]

The European Data Protection Board (EDPB), which is established under article 68 of GDPR, has issued various guidelines and recommendations on the transfer of personal data pursuant to its powers under article 70 of GDPR. These include:

- Guidelines 2/2018 on derogations of article 49 under Regulation 2016/679: These guidelines provide guidance on the application of article 49 of GDPR on derogations for transfer of personal data to third countries.[100]
- Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies: The guidelines set out the expectations of the EDPB on the safeguards required to be put in place by a legally-binding and enforceable instrument between public bodies or by provisions to be inserted into administrative arrangements between public bodies.[101]
- Guidelines 04/2021 on Codes of Conduct as tools for transfers: The guidelines specify the application of article 40(3) of GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data in line with article 46(2)(e) of GDPR.[102]
- Guidelines 05/2021 on the interplay between the application of article 3 and the provisions on international transfers as per chapter V of GDPR: The purpose of the guidelines is to assist data controllers and processors with identifying whether a processing operation constitutes a transfer to a third country or to an international organization, and whether they would therefore have to comply with the provisions of chapter V of GDPR.[103]
- Guidelines 07/2022 on certification as a tool for transfers: These guidelines provide practical guidance on the application of article 46(2)(f) of GDPR on transfers of personal data to third countries or to international organisations on the basis of certification.[104]
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: The EDPB adopted the recommendations to help data exporters with the task of

99 GDPR (n 93) art 49.
100 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (accessed 31 March 2023).
101 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf (accessed 31 March 2023).
102 https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (accessed 31 March 2023).
103 https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (accessed 31 March 2023).
104 https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (accessed 31 March 2023).

assessing third countries and identifying appropriate supplementary measures for protection of personal data.[105]

- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (art 47 of GDPR): These recommendations are meant to, among other things, provide a standard form for the application for approval of binding corporate rules for controllers.[106]

One of the critiques of the adequacy decision approach provided for in GDPR is that it may be difficult to find the required adequacy for cross-border data transfer which proposes the inevitable doubts over the effectiveness and suitability of adequacy decision as an instrument to authorise such data transfer.[107] Another critique is that the approach presents developing countries with a dilemma where, if they seek an adequacy decision, they should have enacted a national data protection law that is in essence, equivalent to that of the EU.[108]

5.2 APEC

The APEC Privacy Framework provides guidance to member economies on the implementation of the Framework, stating that they should have regard to the following basic concept in considering the adoption of measures designed for domestic implementation of the APEC Privacy Framework: Personal data should be processed in a way that protects data subjects' privacy and allows the data subjects and economies to maximise the benefits of data flows within and across borders and that, consequently, as part of establishing or reviewing their privacy protections, member economies should take all reasonable and appropriate steps to identify and remove unnecessary barriers to data flows and avoid the creation of any such barriers.[109]

With regard to cross-border privacy mechanisms, the Framework states that member economies have developed the Cross-Border Privacy Rules (CBPR) system, which provides a practical mechanism for participating economies to implement the APEC Privacy Framework in a cross-border context, and to provide a means for organisations to transfer personal data across borders in a

105 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (accessed 31 March 2023).

106 https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplicationform_en.pdf (accessed 31 March 2023).

107 S Chen 'Cross-border data transfer after Schrems II: The globalisation of EU standards of data protection through adequacy decisions or trade agreements?' Lund University, https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9050792&fileOId=9050794 (accessed 30 September 2023).

108 C Gay 'The GDPR's effect on transatlantic relations' University of Chicago Law School, The GDPR's Effect on Transatlantic Relations (uchicago.edu) (accessed 30 September 2023).

109 https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (accessed 31 March 2023).

manner in which individuals may trust that the privacy of their personal data is protected.[110]

The APEC Cross Border Privacy Rules system, endorsed by APEC leaders in 2011, is a voluntary accountability-based scheme to facilitate privacy respecting personal information flows among APEC economies.[111] There currently are nine participating economies in the CBPR system: Australia, Canada, Mexico, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America.[112]

On cross-border transfer, the Framework states that a member economy should refrain from restricting cross-border flows of personal data between itself and another member economy where the other economy has in place legislative or regulatory instruments that give effect to the Framework or sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it. Further, any restrictions to cross-border flows of personal data should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross-border transfer.[113]

Some of the limitations identified in relation to the APEC CBPR system include that it is voluntary and, therefore, non-binding, and that there is a lack of clarity in what the system will achieve given that it does not supersede national data protection laws.[114]

6 A case for the continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa

One of the main obstacles to cross-border data transfers in Africa is the fragmented and divergent national mandates concerning the collecting and processing of personal data. The presence of multiple data protection regulations that are applicable may lead to ambiguity for governments, businesses and individuals,

110 https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (accessed 31 March 2023).
111 http://cbprs.org/about-cbprs/ (accessed 31 March 2023).
112 http://cbprs.org/government/ (accessed 31 March 2023).
113 https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (accessed 31 March 2023).
114 https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed 30 September 2023).

making it unclear which rules pertain to a particular cross-border data transfer.[115] More specifically, certain nations implement local storage requirements (referred to as data sovereignty or data protectionism) with the specific aim of compelling data to be stored and retained within their borders. In Botswana, only two African countries have received approval for transferring personal data, and in Côte d'Ivoire, regulations for cross-border data transfers mandate that the recipient country must ensure a level of protection that is equal to or greater than that of the originating country.

Further, while most countries, such as Botswana, Cape Verde, Eswatini, Nigeria, São Tomé and Príncipe, South Africa, Uganda and Zimbabwe, provide for transfer of personal data on the basis of adequate level of protection in the recipient country, and some even go a step further to set out the factors that should be considered in determining this adequacy. It is unclear what would qualify as adequate. It is possible that some jurisdiction may not require a high level of compliance, which may lead to difficulties in determining what is adequate. As such, it is imperative for African nations to collaborate in establishing standardised criteria for evaluating sufficient levels of protection.

A number of nations also permit jurisdictional personal data flows if an organisation has put up appropriate security measures, but does not expound on what would amount to appropriate safeguards. Kenya allows for cross-border data transfers if appropriate safeguards are in place. Such safeguards can come in the form of an agreement binding the recipient of data, providing protection for personal data equivalent to that provided by the Kenyan Data Protection Act and Regulations. Alternatively, a transfer may be allowed if the data controller has concluded that appropriate safeguards exist to protect the data. The Regulations, however, do not provide a format of the binding instrument, contrary to the EU approach that provides template standard contractual clauses. It is necessary for African countries to have a harmonised framework in place that would assist in the determination of what would constitute appropriate safeguards.

The growing amounts of data being transferred across borders in Africa underscore the necessity for a flexible and unified system that can handle both current and future data exchanges. This system should take into account variations in local laws, acknowledge commonalities among local regulations, safeguard individual rights, and ensure effective enforcement in case of any breaches. Hence, to promote collaboration among African nations on protecting personal data, it is essential to consider various avenues. These include establishing regional cross-border data frameworks with adequacy assessments; implementing a safe harbour framework; and incorporating suitable data protection measures.

115 Organisation for Economic Cooperation and Development (n 33) 30.

Under the white list or adequacy decisions approach, each country creates a white list of approved countries with adequate data protection measures, and requires that cross-border data transfers be covered by protective contracts. By setting a common standard for data protection, this approach can facilitate the harmonisation of privacy laws across the continent and promote bilateral trade negotiations. Ultimately, achieving a degree of commonality in data protection principles is key to enabling smooth cross-jurisdictional data transfers between jurisdictions with differing data protection laws. The harmonisation of data protection rules on cross-border transfer of data starts from the local and the regional context. This means that locally African countries must borrow and apply certain applicable concepts and guidelines contained in other international regional frameworks.[116] Given this effort, it is essential that there be greater convergence between the specific ways in which countries approach the regulation of data transfers.

On the contrary, the safe harbour framework, originally developed through negotiations between the United States of America and the European Commission, aims to establish an efficient mechanism for businesses operating in a region with limited data protection regulations to transfer data to another jurisdiction with more robust data protection rules and safeguards in place. In Africa, a possible implementation could involve companies seeking safe harbour certification by aligning their privacy practices with the safe harbour privacy principles, as determined by the AU. They would then be required to submit a self-certification form to the relevant regional authority, which may be the AU or a regional bloc. Additionally, companies would need to make their safe harbour privacy policy accessible to the public, clearly demonstrating their commitment to complying with the privacy principles.[117]

Moreover, as the AfCFTA continues to gain momentum and evolve as a central pillar of the continent's economic landscape, it not only is prudent but also imperative to recognise and proactively tackle the intricate issue of cross-jurisdictional data transfers arising from trade agreements. Incorporating provisions pertaining to cross-border data transfers into trade agreements is not a novel concept but rather an essential and forward-looking strategy. By doing so, African nations can harness the synergistic potential that exists at the intersection of digital commerce and cross-border trade. This approach ensures that the benefits of AfCFTA extend seamlessly into the digital realm, fostering an environment conducive to innovation, efficiency and economic growth.

Acknowledging and addressing cross-border data transfers within trade agreements also underscores Africa's commitment to embracing the opportunities presented by the digital age. It reinforces the continent's resolve to

116 United Nations Development Programme (n 9).
117 Hunton & Williams (n 39).

be at the forefront of shaping the future of global trade, where data flows play an increasingly pivotal role. By proactively integrating data transfer considerations into trade accords, African nations demonstrate their readiness to engage in the global digital economy on equal terms, fostering an environment of trust and collaboration with international partners.

7 Conclusion

In conclusion, Africa finds itself at a pivotal juncture on its transformative path into the digital age, with cross-border data transfers serving as a linchpin of this profound journey. The unimpeded circulation of data across borders possesses the extraordinary potential to unlock unparalleled economic prospects and usher in new horizons for businesses and visionary entrepreneurs across the continent. Nonetheless, the absence of a harmonised legal framework for governing these data transfers has cast formidable hurdles and stymied the digital economy's expansion within Africa.

It is imperative that the AU assumes a leading role in the formulation of a comprehensive continental legal framework – one that deftly balances the imperatives of data protection and privacy with the boundless opportunities afforded by an unrestrained digital economy. The economic growth prospects are monumental should African nations unite in harnessing the advantages of cross-border data transfers. To surmount these challenges, seamless cooperation between African governments and regional entities becomes a pressing necessity, with the aim of establishing a uniform legal framework for these data transfers. This framework should be meticulously calibrated to safeguard data integrity and privacy, while concurrently reaping the dividends of an unbridled digital economy. By doing so, Africa can fully harness the potential of its burgeoning digital economy, thus sculpting a prosperous future for its citizens.

In the swiftly-evolving digital landscape, time stands as an unforgiving arbiter. African nations must act expeditiously in orchestrating a harmonised legal framework for cross-border data transfers, positioning themselves as trailblazers in the global digital arena. Failing to do so carries the perilous risk of relegating Africa to a backseat in the digital era, forfeiting the colossal economic and societal advantages inherent in digital transformation. As a renowned data analyst astutely noted, 'data is like the air we breathe. We don't think about it until it's not there.' Much like clean air is indispensable for human survival, the uninterrupted flow of data within a harmonised framework is imperative for Africa's economic prosperity and all-encompassing development.