



# TRANSBORDER DATA FLOWS (TDF) IN AFRICA: THE SNAKES AND LADDERS

Olumide Babalola





# Table of Contents

- 1. **INTRODUCTION** ..... 5
- 2. **TDF DEFINED** ..... 7
- 3. **BARRIERS TO TDF IN AFRICA (The Snakes)** ..... 9
  - a. Data Protection and privacy legislation ..... 10
    - i. Adequacy requirements ..... 11
      - 1. Adequacy standards under regional instruments ..... 11
      - 2. Adequacy standards under national laws ..... 13
  - b. Data localization legislation ..... 16
- 4. **RECOMMENDATIONS AND SOLUTIONS (The Ladders)** ..... 18
  - a. Uniform regulatory approach ..... 19
  - b. TDF Mechanism/ Tools ..... 20
    - i. Standard Contract Clauses ..... 20
    - ii. Binding Corporate Rules ..... 21
  - c. Improved Cooperation Between African DPAs ..... 21
  - d. Adoption of the right to privacy as a fundamental right..... 22
- 5. **CONCLUSION** ..... 23

# About the Author



Olumide is a member of the Nigerian Bar Association, International Bar Association, Chartered Institute of Arbitrators (UK), International Association of Privacy Professionals (IAPP), International Network of Privacy Law Practitioners and Privacy Law Scholars Network, British Nigeria Law Forum, Internet Society, World Litigation Forum, Lawyers Assisting Workers.

## Biography

Olumide Babalola\* is a consummate and passionate digital rights, privacy and data protection lawyer in Nigeria. He holds a Masters' degree in International Commercial Law with ICT & Commerce from the University of Reading, United Kingdom and is currently a PhD candidate at the University of Portsmouth, United Kingdom where he is conducting extensive research on the concept of privacy within the jurisprudence of Nigerian courts.

Olumide's pioneering litigious work around privacy and data protection has seen him litigate the subject up to the Supreme Court of Nigeria and the Community Court of Justice (ECOWAS). In demonstrating his knowledge and expertise in data protection, he handled the first Court of Appeal decision on data protection in the case between Digital Rights Lawyers Initiative and National Identity Management Commission (2021) LPELR – 55623(CA) where the court extensively identified the nexus between data protection and right to privacy under the Nigerian Constitution – the case has become a focal point for all discussions on data protection within legal circles in Nigeria since September 2021.

In 2019, while pursuing his desire to grow data protection law and practice in Nigeria, Olumide co-founded Digital Rights Lawyers Initiative (DRLI) as a civil society and network of lawyers with the principal objective of promotion of digital rights – the intersection of law and technology in Nigeria especially. Up to date, DRLI has litigated more than 50 digital rights cases in court with a large percentage bordering on data protection and privacy under Olumide's direct or otherwise supervision.

In academics, Olumide has 6 published law books to his credit: The Attorney General: Chronicles and Perspectives (2013); Casebook on Labour and Employment Law (2014); Casebook on Corporate Law and Practice (2014); Babalola's Law Dictionary (Of Judicially Defined Words and Phrases 1st and 2nd edition (2018 & 2019); Casebook on Data Protection (2020); Privacy and Data Protection Law in Nigeria (2021).


---

\* PhD Candidate, University of Portsmouth, United Kingdom.

# Abstract

Technology-based transactions are inseparable from the routine exchange of (personal and non-personal) data. These exchanges may not ordinarily pose multiple privacy problems until the movement takes extra-territorial turns thereby facing varying levels of cross-border (disguised) safeguards from compromise and other ills. Between the 70s and 80s frequency of transfer of personal data beyond geographical boundaries in Europe precipitated the regulation of transborder data flows (TDF) beginning with the enactment of the Organization for Economic Cooperation and Development Guidelines in Protection of Privacy and Transborder flows (TDF) of Personal Data (OECD Guidelines) in 1980.

In Africa, the concept of transborder data flows (TDF) is more complex than usually viewed by the stakeholders and this is partly because neither the African Union (AU) nor other regional bodies have introduced operational policies or legislation on TDF. Like many concepts in data protection, TDF is bereft of a generally acceptable legislative or academic meaning. Regardless of the uncertainty, this paper approaches TDF as the transmission of personal data from one country to another country or international entity for the purpose or processing or intended processing. The paper discusses some definitions of TDF - a European concept - as (not) understood within the context of African regional and national data protection legislation. In a comparative and normative approach, the paper analyses the barriers to TDF in Africa vis a vis the European experience and then concludes with relatable recommendations for workable TDF within and outside the African continent from an African perspective beginning with the harmonization of existing regional legislation.



# Introduction

Globalization of trade and commerce is not necessarily a new feature in the world order. It has evolved since the 16th century but assumed a more complex, interconnected and evolving dimension when technology became an inseparable part of every commercial activity.<sup>1</sup> International trade and the utility of personal data are intrinsically inseparable. (Personal) data, especially in highly technologically driven economies have understandably become the 'lifeblood' of economic development and attainment of system goals in our societies.

During the simplest of international transactions, varying types of personal data are routinely exchanged giving rise to user privacy concerns and governmental data sovereignty measures to regulate the international movement of personal data together with the transactions. Attempts to regulate TDF have drawn the ire of Heintz who admonished governments to:



1 Ron Martin et al, 'Globalization at a Critical Conjunction' (2018) 11 Cambridge Journal of Regions, Economy and Society, 3-16.

2 Graca Carvalho et al, 'Themes in Data Strategy: Thematic Analysis of a European Strategy for Data' (EC) (2022) 2 AI and Ethics, 53-63; see also Dan Jerker Svantesson, 'The Concept of Data Privacy Law and Its Application to the Internet' (2014) 27(1) Vox Juris, 185-211.



“Be cautious with data flow controls: the liabilities they bring may outweigh the disadvantages for the coverlines involved”.<sup>3</sup>

In spite of the enormous gains of seamless and free flow of personal data across borders, respective African governments like their European counterparts have mounted regulatory and statutory roadblocks to check and, in some instances, hinder transborder data flow (TDF)<sup>4</sup> on the continent.<sup>5</sup>

Conversations around TDF in Africa have begun since 1985 Conference of African Heads of State and Governments.<sup>6</sup> The numerous economic and socio-political benefits of trans border data flows (TDF) in Africa undoubtedly favour open and unrestricted data transfers across borders from business perspective. As of 2022, out of 54 African countries, 33 have enacted either data protection laws or data localization regulations to check indiscriminate movement of personal data within and outside the African continent.

This paper is divided into four parts. The first examines legislative and (non) academic descriptions and definitions of TDF irrespective of the nomenclature preferred by the authors. The second part discusses the various legislative and technical roadblocks and conditions imposed on TDF in Africa at regional and national levels. In doing this, the paper considers the role of any Pan African and (sub)regional instruments, without prejudice to their legislative force in stifling free flow of data within and outside the continent.

In the third part, the paper makes bespoke recommendations for lawful and safer TDF in Africa. Drawing inspiration from the practices in Europe, the paper suggests customized panacea to the peculiar circumstances on the continent. The fourth part concludes that our quest to find African solutions to Africa’s problems, should begin with harmonization of divergent laws on data protection in Africa and ultimately adopt and recognize privacy as a fundamental right on the continent.

---

<sup>3</sup> Alden Heintz ‘The Dangers of Regulation’ (1979) 29(3) *Journal of Communication*, 129.

<sup>4</sup> The term ‘transborder data flows’ has been used interchangeably with cross border transfer, international transfer of personal data, cross border data flow, transnational data flow, transfer to third country etc.

<sup>5</sup> Nigel Cory et al, ‘How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost and How to Address Them’ (2021) <<https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>> accessed 6 July 2022.

<sup>6</sup> See Declaration of Yamoussokro: Conference on Information’s and Sovereignty, A Contribution to the Lagos Plan of Action, TDR May 1985 at 252-53: see also Olga Estadella – Yuste, ‘Trans border Data Flows and the sources of Public International Law’ (1991)16(2) *North Carolina Journal of International Law and Commercial Regulation*, 430.

## 2. TDF DEFINED

The contemporarily fragmented, ubiquitous and networked nature of production and distribution of goods and services continue accentuate the essentiality of TDF across geographical borders.<sup>7</sup> Admittedly TDF is a European concept, hence every (non)academic inquisition into its meaning must necessarily be traced to foreign actors and resources.

Bu-Pasha describes TDF as a scenario which involves collection of data by a controller for onward transmission to another controller or processor based in another country.<sup>8</sup> Even though Kuner did not offer a conclusive definition, he decries the lack of adequate legislative and academic guidance or precision in the meaning of cross border transfer. He notes that the fuzziness is also made evident by distortion between data transfer and mere transit under EU data protection law.<sup>9</sup>

Faced with similar circumstances, Branscomb also blames the uncertainty hovering on the meaning of TDF on the divergent definitions ascribed to the concept by varying authors.<sup>10</sup> In her review of definitions of TDF, she found: ‘electronic movement of data between countries’<sup>11</sup> ‘units of information coded electronically for processing by one or more digital computers which transfer or process the information in more than one nation-state.’<sup>12</sup> Hardy defines TDF as ‘the transmission of data or information over national boundaries’ even though the definition falls short of other nuances of the concept especially since mere transit does not necessarily constitute TDF under the GDPR.<sup>13</sup>

Ultimately, since various research and legislation continue to provide divergent definitions of TDF, it has become apparent that the complexity and uncertainty of the term will vary from jurisdiction to jurisdiction. While the EU Data Protection Directive addresses rather than define

---

<sup>7</sup> Sventlana Yakovleva, ‘Personal Data Transfers in International Trade and EU Law: A Tale of Two ‘Necessities’ (2020) 21 *Journal of World Investment and Trade*, 881-919.

<sup>8</sup> Shakila Bu-Pasha, ‘Cross border Issues Under EU Data Protection Law with Regards to Personal Data Protection’ (2017) 26(3) *Information and Communications Technology Law*, 213-223.

<sup>9</sup> See article 4(1)(c) EU Data Protection Directive and Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, Oxford, 2013) 15.

<sup>10</sup> Anne W. Branscomb, ‘Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition’ (1983) 36(4) *Vanderbilt Law Review*, 990.

<sup>11</sup> W.L. Fishman, ‘Introduction to Transborder Data Flows’ (1980) 16 *Stanford Journal of International Law*, 1.

<sup>12</sup> Eric Novotny, ‘Transborder Data Flows and International Law: A Framework for Policy-Oriented Inquiry’ (1980) 16 *Stanford Journal of International Law*, 141.

<sup>13</sup> I. Trotter Hardy, ‘Transborder Data Flow: An Overview and Critique of Recent Concerns’ (1983) 9 *Rutgers Computer & Technology Law Journal*, 247.

TDF as ‘transfer to a third country’<sup>14</sup> of personal data, the OECD Privacy Guidelines defines the term as ‘movement of personal data across national borders.’<sup>15</sup>

In *Bodi Lindquist case*<sup>16</sup> the European Court of Justice (ECJ) rather than define TDF, only confined its decision to what does not constitute TDF under the EU Data Protection Directive and the need for adequate level of protection.<sup>17</sup> The GDPR defines the broader term ‘cross border processing’<sup>18</sup> but approaches TDF as ‘transfers of personal data which are undergoing or are intended for processing after transfer to a third country or to an international organization’.<sup>19</sup> In the African context, neither the Malabo Convention<sup>20</sup> nor the ECOWAS Act<sup>21</sup> defines cross border transfer of data, even though both instruments make similar provisions on TDF. However, the SADC Model Law defines ‘trans-border flow’ of personal data as ‘any international flow of personal data by the means of electronic transmission or any other transmission means including data transmission by satellite.’<sup>22</sup> As much as this definition appears a face-saving one, the soft law is not binding, and its intervention is not watertight to resolve conflicts that arise with respect to the regular requirement and conditions for TDF. For example, will the ‘flow’ of personal data on the Internet qualify as TDF under this provision? Also, will be internal flow of data within a company’s subsidiaries based in other countries constitute international flow of data under this definition?.

SADC Model Law’s definition appears to have been inspired by a 1976 United States Congressional document which defines TDF as ‘electronic transmission of data across political boundaries for process and storage in computer files’.<sup>23</sup> This attempt is not however without its own teething problems especially with the introduction of political considerations since the

---

<sup>14</sup> See article 25 Directive 95/46/EC which was enacted in October 1995 by the EU to predominantly regulate the free flow of personal data within the union.

<sup>15</sup> OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, part I.

<sup>16</sup> C-101/01(2003) ECR-I-12971

<sup>17</sup> The court noted that, publication of personal on the Internet does not constitute TDF even if it can be accessed in countries outside the EU.

<sup>18</sup> As ‘processing of personal data in more than one EU members state by controller with establishment in more than one member state or processing by controller in one member state which affects data subjects in more than one member state.’ See GDPR, art. 4 (23).

<sup>19</sup> General Data Protection Regulation, art. 44.

<sup>20</sup> African Union (AU) Convention on Cyber Security and Personal Data Protection.

<sup>21</sup> Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS.

<sup>22</sup> Southern African Development Community (SADC) Model Law, part I, art. 1(21).

<sup>23</sup> See United States Congress, House Committee on Interstate and Foreign Commerce, 96<sup>th</sup> Congress, 1<sup>st</sup> session, 1979 International Barriers to Data Flows: Staff Background Report, Government Printing Office, Washington DC, 1982; see also Gisela Moohan et al, Trans border Data Flow: A Review of Issues and Policies’ (2007)37(3) Library Reviews, 27.

Model law is a soft law with no binding effect even though researchers have argued that its influence on data protection legislation within the sub-region is undeniable.<sup>24</sup>

Hence, from an aggregate of academic, legislative and policy interventions, TDF is the movement, exchange or flow of personal data between entities across political and geographical boundaries for the purpose of processing or intended processing.<sup>25</sup>

While a number of data protection legislation by African countries completely omit the definition of TDF in their national laws<sup>26</sup>, a few provide variants of definitions for the term. Omission of definition of the concept will breed more interpretation and enforcement problems than the already identified ones. Of all the francophone African countries that have enacted national data protection legislation only the Botswanan law defines the term ‘transborder flow’ as the ‘international flow of personal data which can either be transmitted by electronic or other forms of transmission including satellite’.<sup>27</sup> Even though, most of the African countries’ data protection laws make provisions bordering on TDF, the enforcement problems always stem from lack of clarity on what nature of processing is covered by the notion.<sup>28</sup>

### 3. BARRIERS TO TDF IN AFRICA (The snakes)

International transfer of data is not a novel phenomenon. However, the ubiquity of Internet-enabled activities has made global transmission of large (personal) data seamless and more cost effective than envisaged by international trade policy makers.<sup>29</sup> These unprecedented technologically driven cross border movement of data often lead to uncontrolled compromise of such personal information in the custody of private and public bodies. Historically, the agitators for international protection of personal data from the increased risks of interference with

---

<sup>24</sup>Christoff Ferreira, ‘Harmonisation of Data Protection Regimes in the Southern African Development Community: Considering the Influence of SADC Model Law on Data Protection and the European Union on Data Protection Laws in SADC’ (LLM Thesis, University of Cape Town 2021).

<sup>25</sup> Processing in this context could mean collection, use, transmission, modification and storage etc. of personal data.

<sup>26</sup> See the national laws of Kenya, Mauritius, Ghana, South Africa, Uganda, Zambia, Rwanda and Nigeria.

<sup>27</sup> Data Protection Act (No. 32 of 2018), section 2.

<sup>28</sup> Complexity of TDF begins from lack of precision with respect to its meaning and ramifications, it is also befitting that EU law distinguishes transfer of data from ‘transit’ see article 4 of the repealed EU Data Protection Directive 95 and also UK Information Commissioner, ‘The Eighth Data Protection Principle and International data transfers’ (30 May 2006), para 1.3.4.

<sup>29</sup> Organization for Economic Cooperation and Development (OECD), Digital Trade and Market Openness (Paris: OECD Trade Policy Papers No. 217, 2018).

personal autonomy and privacy began in the 70's when the information society<sup>30</sup> became internationalized.<sup>31</sup>

In spite of the enormous economic benefits of free flow of data across borders, some African countries like their Europeans counterpart place certain legislative roadblocks against TDF based on privacy, security, mercantilist or protectionist concerns. Walden notes that TDF generally involves varying kinds of personal data exchanged along with non-personal data within four major contexts, to wit: intra-company information (i.e group of companies/parent companies and subsidiaries based in different countries), intra-company information, governmental information needs and transnational pursuit of information.<sup>32</sup> In analysing the dilemma surrounding regulation of TDF, Bothe identifies three main interests exhibited by the data subjects, controllers, & policy makers as: access to information, access to market and desire for control.<sup>33</sup>

### **3.1 Data Protection and Privacy Legislation**

(Personal) data is the lifeblood of international trade and other economic interactions. The optimal use of (personal) data facilitates economic growth and advancement. Conversely, the misuse of personal data within the context its international flow has led to the regional and national enactment of data protection laws to check TDF and for other purposes. On one hand, TDF has been happily referred to as 'commerce-enabling hallmarks of 21<sup>st</sup> century globalization'<sup>34</sup> and the connectivity tissue holding the global economy together<sup>35</sup> yet in another account, Grossman laments that 'one of the salient characteristics of the TDF issue is the rapidity with which it has become a problem of major concern'.<sup>36</sup> In a bid to arrest the circumvention of national interests for corporate gains by taking advantage of the unsupervised or unregulated

---

<sup>30</sup> This is an idea of self-regulation on issues of privacy, trust, security, copyright etc. for the development of the field of robotics and artificial intelligence by some mathematicians, scientists and engineers which began post World War II. See Robin Mansell, 'The Life and Times of the Information Society' (2010) 28(2) *Prometheus*, 165-185.

<sup>31</sup> Peter Blume, 'Transborder Data Flow: Is There a Solution in Sight?' (2000) 8(1) *International Journal of Law and Information, Technology*, 65-66.

<sup>32</sup> Lan Walden and Nigel Savage, 'Trans border Data Flows' in Chris Edwards, Nigel Savage and Lan Walden (eds) *Information and Technology Law* (Palgrave Macmillan, London, 1990) 121.

<sup>33</sup> Michael Bothe, 'Transborder Data Flows: Do We Mean Freedom or Business?' (1989) 10(2) *Michigan Journal of International Law*, 333.

<sup>34</sup> W. Gregory Voss, 'Cross- Border Data Flows, the GDPR and Data Governance' (2020) 29(3) *Washington International Law Journal*, 486.

<sup>35</sup> Susan Lund et al, 'Globalization Is Not in Retreat: Digital Technology and the Future Trade' (2018) 97(3) *Foreign Affairs*, 130 -140.

<sup>36</sup> Garry S. Grossman, 'Trans border Data Flow: Separating the Privacy Interest of Individuals and Corporations' (1982) 4(1) *Northwestern Journal of International Law & Business*, 2.

international flow of personal data, the EU adopted the GDPR to ease free flow of data across member states subject to certain safeguards. i.e. adequacy requirement, binding corporate rules etc.<sup>37</sup>

### ***3.1.1 Adequacy requirements***

The assessment of ‘adequate level’ of data protection legislation existing in a certain jurisdiction became a standard in the EU via the Data Protection Directive 95. By this requirement, conditions are imposed for transfer of personal data to countries ruled to have fallen short of the ‘adequacy’ standards.<sup>38</sup> In the EU, decisions on adequacy level of data protection practices of a country (adequacy decisions) are made by the European Commission as published in its journal or website.<sup>39</sup> The adequacy standard under the GDPR evaluates the jurisdiction’s index of respect of rule of law, independence of its supervisory authority, and international commitment to development of data protection.<sup>40</sup>

In Africa, admittedly, the framework for adequacy standards or requirement or decision is not regionally institutionalized, but such provisions however exist in the regional instruments and national legislation albeit with diverse considerations, effect, and enforcement mechanisms.

#### *a. Adequacy standards under regional instruments*

The Malabo Convention was predominantly adopted in 2014 by the AU for the regional harmonization of cyber security and data protection governance on the continent.<sup>41</sup> The convention does not define the parameters of TDF but it regulates such flows within and outside

---

<sup>37</sup> Mira Burri, ‘The Reform of the EU Data Protection Framework: Outlining Key Changes and Accessing Their Fitness for a Data-Driven Economy’ (2016) 6 Journal of Information Policy, 479-511.

<sup>38</sup> Jennifer Stoddart et al, ‘The European Union’s Adequacy Approach to Privacy and International Data Sharing in Health Research’ (2016) 44(1) Journal of Law, Medicine & Ethics, 143-155.

<sup>39</sup> General Data Protection Regulation, article 45 (8); and Peter Blume, ‘EU Adequate Decisions: The Proposed New Possibilities’ (2015) 5(1) International Data Privacy Law, 35. In 2010, the adequacy assessment under the EU Data Protection Directive turned negative in a unilateral assessment carried out by the European Commission on four African Countries to wit: Mauritius, Tunisia, Burkina Faso, Morocco. See Alex B. Makulilo, ‘Data Protection Regimes in Africa: Too Far from the European ‘Adequacy Standard’ (2013) 3(1) International Data Privacy Law, 42-50.

<sup>40</sup> General Data Protection Regulation, article 45(2).

<sup>41</sup> Kaitlin Ball, ‘Introductory Note to African Union Convention on Cyber security and Personal Data Protection’ (2017) 56(1) International Legal Materials, 164-192.

the AU where a ‘third country’<sup>42</sup> or international entity’s data protection adequacy level is not formidable enough to guarantee protection to data subjects when their rights and freedoms are violated or threatened.<sup>43</sup> The provision however excuses adequacy requirements where a national data protection authority (DPA) authorizes such transfer although the provision is bereft of factors to be considered before such authorizations.<sup>44</sup>

Even though the Malabo Convention is a Pan-African instrument, it does not currently constitute a direct barrier to TDF on its own by reason of article 36 which suspends its enforcement until ratified by 15 member states.<sup>45</sup> However, in its comatose state, the Malabo Convention continues to indirectly influence national data protection laws in Africa with or without direct reference in such laws. For example, the Nigeria(n) Data Protection Regulation (NDPR) and its Implementation Framework expressly rely on the convention to remedy any defect in the Nigerian regulation.<sup>46</sup> The Kenyan Data Protection Act also mandates the Data Commissioner’s office to ensure the country’s compliance with international conventions and agreements in contemplation of the Malabo Convention.<sup>47</sup>

Unlike Malabo Convention, the ECOWAS Act is immediately enforceable upon ratification and domestication by respective member states within the sub region.<sup>48</sup> The ECOWAS Act was adopted four years before the Malabo Convention and the Act has been reputed as a source of inspiration to the convention.<sup>49</sup> The ECOWAS Act is reputed as the ‘only binding regional/international data protection’ instrument in force in Africa<sup>50</sup> and it is supplemented by

---

<sup>42</sup> The term ‘third country’ is not also defined in the convention.

<sup>43</sup> African Union (AU) Convention on Cyber security and Personal Data Protection, article 14(6) (a).

<sup>44</sup> African Union (AU) Convention on Cyber security and Personal Data Protection, article 14 (6) (b).

<sup>45</sup> As of July 2022, only 8 countries have ratified the convention: Chad, Comoros, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome, Principe and Zambia. See also Uchenna Orji, ‘The African Union Convention on Cyber Security: A Regional Response towards Cyber Stability?’ (2018) 12(2) Masaryk University Journal of Law and Technology, 91.

<sup>46</sup> Olumide Babalola ‘Nigeria’s Data Protection Legal and Institutional Model: An Overview’ (2021) 00(0) International Data Privacy Law, 1. Greenleaf regards the Malabo Convention as ‘potentially most important development in Africa’s data protection framework’, see Graham Greenleaf et al ‘International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis’ (2022) 44 Computer Law and Security Review, 9.

<sup>47</sup> Act No. 24 of 2019, section, 8(1)(i).

<sup>48</sup> It was signed in Abuja, Nigeria on the 16<sup>th</sup> day of February 2010 by Benin, Burkina Faso, Cape Verde, Cote d’Ivoire, Gambia, Ghana, Guinea Bissau, Mali, Nigeria, Sierra Leone and Togo.

<sup>49</sup> Dennis Agelebe, ‘Implementation of the ECOWAS Supplementary Act on Personal Data Protection: Lessons from the EU GDPR’ (2020) 4(1) Journal of Data Protection & Privacy, 1-18.

<sup>50</sup> Greenleaf (n 44) 14.

provisions of the ECOWAS Directive on cybercrime.<sup>51</sup> In regulating TDF, the scope of ECOWAS Act is limited to member states i.e personal data can only be freely moved outside the ECOWAS region where the recipient country provides adequate level of privacy protection. As with the Malabo Convention, the ECOWAS Act is also bereft of clarity on meaning of TDF, parameters of adequacy or information on adequacy decisions and how they are made. These omissions make the entire framework contemplated by the Act insufficient to ease or regulate TDF within and outside the subregion.<sup>52</sup> In the absence of such legislative guidance on adequacy conditions and decisions, TDF legal framework under the Act remains academic and abstract.

From the foregoing, the extent to which the ECOWAS Act constitutes barrier to TDF in Africa is highly debatable only to the extent of its influence on subsequently enacted national data protection laws in Africa. Happily, the SADC Law defines TDF but it is a soft law with merely persuasive effect. Hence, it is not considered as a barrier here.

*b. Adequacy under national laws*

Countries with weaker data protection legal framework experience reduced transit of data to and from EU countries as a result of the stringent European data privacy legal system.<sup>53</sup> Hence, enforcement of data privacy laws negatively impact TDF and consequently development of economic ties between African countries and their European counterparts.

Undoubtedly, the African data protection legal regime is fashioned after the European template together with foreign but incompatible enforcement mechanisms. Mannion notes that the GDPR-styled data protection legislation may not yield similar effects in Africa for many reasons. e.g. lack of Africa-wide comprehensive legislation, non-independence of DPAs, ineffective justice delivery systems, issues with technological expertise e.t.c.<sup>54</sup> On the same wavelength,

---

<sup>51</sup> The Directive C/DiR. 1/08/11 on fighting cybercrime within the ECOWAS was signed on the 19<sup>th</sup> day of August 2011 to provide framework for 'efficient and reliable international cooperation'.

<sup>52</sup> Unlike the GDPR, the ECOWAS Act is silent on factors to be considered for adequacy decision as well as the body responsible for such decision. Within the context of TDF, adequacy decision is distinguishable from supervisory authority's approval or authorization.

<sup>53</sup> Mona Farid Badran et al, 'Economic Impact of Data Localization in 5 selected African Countries, An Empirical Study' < [https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC\\_RANITP\\_Economic\\_Impact\\_of\\_Data\\_Localization\\_in\\_5\\_selected\\_African\\_Countries.pdf](https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_Localization_in_5_selected_African_Countries.pdf) > accessed 15 July 2022.

<sup>54</sup> Cara Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets' (2020) 53(2) Vanderbilt Journal of Transnational Law, 695.

Slokenberga also agrees that the two (fundamentally divergent) systems are not comparable.<sup>55</sup> While analyzing a report of adequacy on four African countries commissioned by the EU in 2010, Makulilo advises that the borrowing of legislative ideas from EU's data protection framework should not be a matter of 'copy and paste'. He stresses that extensive public consultation and debates on the workability of such importation vis a vis its peculiarity must be had.<sup>56</sup>

Nevertheless, whether as a thoughtless transplantation of a foreign notion, cerebral protectionist moves or genuine humanitarian attempts to preserve citizens' personal autonomy, African governments and policymakers have replicated the European concept of adequacy into the fabrics of their data protection legal regime. However, with or without wholesale transplantation, adequacy decisions in Europe have a snowballing effect on call at governance in Africa. For instance, in July 2022, the Court of Justice of the European Union (CJEU) declared the EU-US Privacy Shield (Safe Harbor Principles)<sup>57</sup> unlawful, having fallen short of adequacy requirements. The effect of this decision is multi-faceted on Africa in its dealings with US and EU.<sup>58</sup> In Africa, right from the Cape Verdean Data Protection Act enacted in 2001, successive African governments have enacted their national laws to include provisions on TDF with varying implications on movement of personal within and outside the African continent. The scattered and irregular approach to TDF in Africa is in itself a barrier to free flow of personal data within and outside the continent. To demonstrate this lack of cohesion and uniformity, I briefly consider the data protection laws of Ghana, Kenya, South Africa, and Rwanda in the light of their provisions on TDF.

In Ghana, the enactment of Data Protection Act<sup>59</sup> was influenced by the country's international economic relationships and commitments, hence its extraterritorial flavor.<sup>60</sup> Surprisingly, out of the Act's ninety-nine sections, none is devoted to TDF. This gives the impression that movement of personal information out of Ghana is not statutorily regulated. The closest

---

<sup>55</sup> Santa Slokenberga et al, 'EU Data Transfer Rules and African Legal Realities: Is Data Exchange for Biobanking Research Realistic?' (2019) 9(1) *International Data Privacy Law*, 30.

<sup>56</sup> Makulilo (n 38) 50.

<sup>57</sup> For comprehensive reading, see Damon Greer, 'Safe Harbor – A Framework That Works' (2011) 1(3) *International Data Privacy Law*, 143.

<sup>58</sup> Gehan Gunasekara 'The "Final" Privacy Frontier? Regulating Trans-Border Data Flows' (2009) 17(2) *International Journal of Law and Information Technology*, 147-179.

<sup>59</sup> Act 843 of 10<sup>th</sup> day of May 2012.

<sup>60</sup> Dominic N. Dagbanja, 'The Right to Privacy and Data Protection in Ghana' in Alex B. Makulilo (ed) *African Data Privacy Laws* (Springer Publishing, Switzerland, 2016) 232.

provision to TDF is found in section 18(2) which seeks to protect foreign data subjects by mandating controllers to comply with the legislation of the jurisdiction where data emanates. Section 30(4) however covers situations where processing is not domiciled in Ghana and the processor concerned is obligated to obey the laws of Ghana. South Africa has been described as the most ‘data restrictive’ country in Africa.<sup>61</sup>

The South African Protection of Personal Information Act (POPIA)<sup>62</sup> to among other purposes, enhance ‘free flow of information within the country and access international borders.’<sup>63</sup> POPIA prohibits TDF except the recipient is ‘subject to a law, binding corporate rules or binding agreement with adequate level of protection.’<sup>64</sup> Unlike most data protection laws elsewhere in Africa, POPIA provides some sort of clarity on the expectations of ‘adequate level of protection’. The Act however permits TDF to a country without adequate protection subject to the supervisory authority’s authorization<sup>65</sup> but what is however missing in the text of the Act is clarity on the body that makes such decision and how it’s made. Regardless of this comparative legislative clarity, in a 2017 Report, Ferracane confirmed that restrictions on TDF has sporadically increased the cost of doing business in South Africa.<sup>66</sup> He further finds that South African has implemented conditional TDF which forbids the movement of certain interiors of data abroad except certain conditions are satisfied.<sup>67</sup>

Kenya’s relatively recent entry into the African data protection landscape with the enactment of Data Protection Act<sup>68</sup> and the establishment of office of Data Protection Commissioner which has hit the ground running is quite commendable. In an unprecedented manner, the Kenyan Act curiously devised TDF restriction as one of its principles of data protection.<sup>69</sup> Hence, Hoofnagle et al have argued that data protection ought to be strategically legislated and practiced to meet

---

<sup>61</sup> Cory (n 5).

<sup>62</sup> Act No. 4 of 2013 but predominantly entered into full operation in July 2020. See Lee Swales, ‘The Protection of Personal Information Act and data de-identification’ (2021) 117(7-8) South African Journal of Science, 1.

<sup>63</sup> POPIA, section 2.

<sup>64</sup> Protection of Personal Information Act, section 72(1).

<sup>65</sup> Protection of Personal Information Act, section 57(1) (d).

<sup>66</sup> Martina F. Ferracane, ‘Restrictions on Cross- Border Data Flows: A Taxonomy’ (2017) ECIPE Working Paper, No. 11/2017.

<sup>67</sup> Martina F. Ferracane, ‘South Africa and Data Flows. How to Fully Exploit the Potential of Digital Economy’ (2018) Discussion Paper, April 2018.

<sup>68</sup> Act No. 24 of 2019.

<sup>69</sup> Kenya Data Protection Act, section 25 (h).

the peculiar demands of respective jurisdictions.<sup>70</sup> The sixth part of the Kenyan Act restricts TDF to jurisdictions in favour of which the Kenyan Data Commissioner has proof of ‘appropriate safeguards’ with respect to data security and protection.<sup>71</sup> Nowhere in the entire Act or the Data Protection (General) Regulations 2021 made pursuant to the principal Act is the term ‘appropriate safeguards’ defined.<sup>72</sup> The Kenyan- Styled TDF restriction is conditional and reported to have damning effect on local production which sector is the biggest beneficiary of data transfers.<sup>73</sup>

In Egypt, the Personal Data Protection Law (PDPL)<sup>74</sup> was enacted to standardize and control data handling and management in the Country thereby drawing its inspiration from EU GDPR.<sup>75</sup> This law requires regulatory approvals for cross-border movement of data.<sup>76</sup> Although the PDPL does not specifically reference adequacy standards, it cautions against TDF in whatever form to any jurisdiction with lower level of data protection than Egypt’s. It adds that before such transfers can be authorized, permits must however be issued by the supervisory authority.<sup>77</sup>

### ***3.2 Data localization legislation***

Across the world, enactment of new data localization laws or enforcement of existing ones is an after-effect of Snowden revelations in June 2003.<sup>78</sup> In contrast to TDF, data localization in this

---

<sup>70</sup> Chris Jay Hoofnagle et al ‘The European Union General Data Protection Regulation: What It Is and What it Means’ (2019) 28 (1) Information and Communications Technology Law, 65-98.

<sup>71</sup> Data Protection Act, section 48 (a); section 48 (c) also makes compliance with data protection principles additional requirement.

<sup>72</sup> The Regulations were issued by the Cabinet Secretary pursuant to section 71 of the Data Protection Act 2019. The Regulations omits definition but specifically subject TDF to ‘data protection safeguards, adequacy decision, necessity and consent’ with more elaborate requirements for qualification. See Part 6, the Data Protection (General) Regulation 2021.

<sup>73</sup> Global Data Alliance, ‘Cross- Border Policies under the US-Kenya Free Trade Agreement’ (June 2020) < <https://globaldataalliance.org/wp-content/uploads/2021/07/06222020uskenyaftacomm.pdf>> accessed 9 July 2022.

<sup>74</sup> Law No. 151 of 2021

<sup>75</sup> Miral Sabry Alashry, ‘Investigating the Efficiency of the Egyptian Data Protection Law on Media Freedom: Journalists’ Perceptions’ (2022) 35(1) Communications and Society, 102-108.

<sup>76</sup> Personal Data Protection Law, article 14; see also United Nations, Digital Economy Report 2021. Cross Border Data Flows and Development: For Whom the Data Flow, 127.

<sup>77</sup> See Alaa Kulaib, ‘Egypt’s Personal Data Protection Law (PDPL) and Where It Stands According to the International Standards’ (2021) < <https://afteegypt.org/en/legislations-en/legislative-analysis-en/2021/08/04/24312-afteegypt.html> > accessed 10 July 2022.

<sup>78</sup> Neha Mishra, ‘Data Localization Laws in a Digital World Data Protection or Data Protectionism’ (2016) The Public Sphere, 137.

context is the entire mechanism employed by governments to hinder digital personal data from moving out of their territorial jurisdiction.<sup>79</sup> Data localization rules dictate where and how personal data must be collected, modified and/or stored with the undesired effect of interference with international flow of data for business efficacy and sundry benefits of globalization.<sup>80</sup> Taking a cue from Europe, African governments often impose data localization requirements for data sovereignty and economic interests disguised as citizens' privacy concerns or data protectionism. Apart from the provisions of extant data protection legislation on TDF in their respective jurisdictions, a number of African countries have gone ahead to enact dedicated data localization laws.<sup>81</sup> Kuner argues that governments' restriction of movement of data abroad is driven by four policy objectives to wit: ensuring compliance with privacy laws, avoiding risks associated with data processing in other jurisdictions, enforcement problems with extraterritoriality of privacy laws, and boosting user confidence.<sup>82</sup>

In Kenya, apart from the Data Protection Act that expressly empowers the Cabinet Secretary to restrict certain data processing activities to servers located in Kenya,<sup>83</sup> there are other far reaching sector specific data localization legislation.<sup>84</sup> To achieve data localization objectives, the Kenyan National ICT Policy mandates 'government data' to be stored in local servers in a bid to ensure Kenyan citizens' data privacy.<sup>85</sup> In similar fashion, both the Kenya Information and Communications (Registration of SIM Cards) Regulations 2015 and Privacy Security Regulation Act, Computer Misuse and Cybercrimes Act 2018 e.t.c. contain data localization provisions which limit the movement of personal data outside Kenya.

Nigeria's most comprehensive data protection (subsidiary) legislation – the NDPR<sup>86</sup> - does not contain express provisions on data localization. However, there are other sector-specific

---

<sup>79</sup> Yanging Hong, 'Data Localization: Deconstructing Myths and Suggesting a Workable Models for the Future. The Cases of China and the EU' (2019) 15(17) Brussels Privacy Hub, Working Paper, 1-29. Data localization is the requirement to store data on servers located within a given jurisdiction' see Theo Lynn et al. *Data Privacy and Trust in Cloud Computing* (Palgrave Macmillan, Switzerland, 2021) 50.

<sup>80</sup> Erica Fraser, 'Data Localization and the Balkanization of the Internet: (2016) 13(3) SCRIPTED, 360.

<sup>81</sup> Nigeria, for example, has a couple sector-specific regulations on data localization.

<sup>82</sup> Christopher Kuner, 'Data Nationalism and Its Discontents' (2012) 64 Emory Law Journal, 2089-2098.

<sup>83</sup> Data Protection Act, section 50.

<sup>84</sup> Malcom Kijah et al, 'Data Protection and Data Localization in Kenya' (2022) Policy Brief 03, Mandela Institute, University of Witwatersrand, South Africa. Processing activities in this context refers to collection, use, transmission and storage which must be domiciled in Kenya.

<sup>85</sup> National Information Communications Technology Policy 2019, paragraph 4.4.

<sup>86</sup> Nigeria Data Protection Regulation (NDPR) was issued in January 2019 to among other objectives, regulate the exchange of personal data of Nigerians.

legislation that speak to data localization in Nigeria.<sup>87</sup> Abdulrauf et al however argue that data localization measures interfere with the rights of Nigerians and ECOWAS citizens to establish businesses.<sup>88</sup> In 2019, Nigeria's erstwhile supervisory authority<sup>89</sup> issued an amended set of Guidelines<sup>90</sup> for the ICT industry. The Guidelines, among other objectives, aim to develop Nigeria's local ICT contents by regulating 'technology transfer, use of indigenous manpower and local manufacturing'. In its data localization drive, the Guidelines mandate all sovereign data to be hosted and stored in local servers<sup>91</sup> Such data can however be hosted outside Nigeria with express permission of the regulator. The Guidelines however omit the definition of sovereign data but this does not detract from its data localization status and objectives as it also mandates telecommunication and ICT companies to host traffic data in the country.<sup>92</sup>

In addition to the Guidelines, the National Cloud Computing Policy, Telephone Subscribers Regulation 2011, Guidelines on Point of sale (POS) Card Acceptance Service Guidelines all have varying provisions mandating local hosting and or storage of certain kinds of personal data within Nigeria.<sup>93</sup> Daily processing users' data across borders by service providers and product suppliers have become a routine and seamless exercise. This technology-enabled service is bedevilled by the somewhat stringent obligations imposed on foreign governments and businesses by EU- styled data protection laws in Africa which harshly hamper TDF between the continent and the west vice- versa leaving the latter with bleeding GDP.

#### 4. RECOMMENDATIONS AND SOLUTIONS (The Ladders)

---

<sup>87</sup> NDPR makes provision for TDF but not necessarily a requirement for certain data to be domiciled in Nigeria. This underscores the distinction between TDF conditions and data localization requirements.

<sup>88</sup> Lukman Abdulrauf and Oyeniyi Abe, 'The (Potential) Economic Impact of Data Localization Policies in Nigeria's Regional Trade Obligations' (Policy Brief of Mandela Institute, University of Witwatersrand, South Africa, 2021).

<sup>89</sup> Since 2019 National Information Technology Development Agency (NITDA) played the role of national supervisory authority in Nigeria upon its issuance of the NDPR but in 2021, the role was transferred to the newly established Nigeria Data Protection Board (NDPB). <<https://techpoint.africa/2022/03/10/nigeria-data-protection-bureau>> accessed 10 July 2022.

<sup>90</sup> Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) (as amended August 2019) <<https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf>> accessed 12 July 2022.

<sup>91</sup> Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) (as amended August 2019), paragraphs 13.1 and 13.2.

<sup>92</sup> (Clause 4).

<sup>93</sup> Abdulrauf (n 87) 1. Adeleke argues that the basis of Nigeria's data localization policies is geared towards suppression of 'negative trade balance in the ICT sector'. See Fola Adeleke, 'Exploring Policy Trade. For Data Localization in South Africa, Kenya and Nigeria: Policy Brief of Mandela Institute University of Witwatersrand, South Africa, 2021 <<https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/PB09%20Trade-offs%20in%20data%20localisation.pdf>> accessed 11 July 2022.

In spite of Africa's dependence on the western world for its economic sustenance, 'African solutions' are still the most preferred or potent for Africa's problems.<sup>94</sup> From an African perspective, privacy, data protection and data localization<sup>95</sup> are borrowed concepts: the African Charter on Human and People's Right (African Charter) does not have any provision on privacy, hence it is (arguably) not a fundamental right at regional level.<sup>96</sup> Hence, importing the concepts into Africa together with their attendant pitfalls must necessarily take cognizance of the continent's peculiarities in terms of fitness for purpose and anticipated results.

#### ***4.1. Uniform regulatory approach***

Currently, since there is no regional governance of TDF since regulation has been in silos and fragmented at the national level in a free-for-all and uncoordinated manner. African governments have taken diverse initiatives to govern TDF based on their whims and patterns as dictated by their legal systems. Some countries do not have data protection legislation, some have but omitted provisions on TDF. For example, the Ghanaian Data Protection Act has no provisions of transfer of data out of the country. Others have adequacy requirements but with varying nomenclature and parameters. For example, while Kenya has 'appropriate safeguards' requirements some francophone countries require registration/authorizations with the supervisory authorities before TDF and others require license/approval of the supervisory authority.<sup>97</sup>

Given the irregular and conflictingly divergent state of data protection laws in Africa, the clog on TDF is not necessarily the existence of data protection laws as it were but the uncertainty of uniform regulation of such international movement across borders. In this regard, Zeller advised

---

<sup>94</sup> Zekeri Momoh, 'African Solution to African Problems: A Critical Approval' (2016) 5(1) *Journal of African Union Studies*, 39-62.

<sup>95</sup> The first recorded idea of Europe-only cloud emerged in 2011, see Christopher Kuner et al, 'Internet Balkanization Gathers Pace: Is Privacy the Red Driver?' (2015) 5(1) *International Privacy Law*, 1-2.

<sup>96</sup> The premium placed on privacy by Africans is further questioned by this far-reaching omission. See Olumide Babalola, *Privacy and Data Protection Law in Nigeria* (Noetico Repertum, Lagos, 2022) 35. It is however curious to know that right to privacy was contained in the first draft of the African Charter. See Yohannes E. Ayalew, 'Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law' (2022) 2(1) *International Data Privacy Law*, 160.

<sup>97</sup> See Olumide Babalola and Gbenga Sesan, 'Data Protection Authorities in Africa: A Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of Their Existence on the Continent' (2021) <<https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf>> accessed 13 July 2022. The Cape Verdean DPA has issued 1307 TDF authorizations since its creation in 2011, see Mercy King' Ori et al 'A look into DPA Strategies in the African Continent' (2022) <<https://fpf.org/blog/fpf-report-a-look-into-dpa-strategies-in-the-african-continent/>> accessed 12 July 2022.

that the solution to such uncertainty is the creation of a ‘half-way house’ in the mould of a global (in this case, regional) law transposed into national laws.<sup>98</sup> In the absence of a unified legal framework for TDF in Africa, businesses will suffer as a result of high cost of compliance with the staggered regulatory requirements across board.<sup>99</sup> Apart from the Malabo Convention which remains comatose, it is advisable for African countries to enter into multi-party agreements on TDF for uniformity of purpose and enforcement within and outside the region.

Needless to say, that since, the GDPR was adopted to harmonize the divergent rules of data protection in Europe at that time, Africa can adopt that approach as well since the EU also have a Convention 108 in the ilk of Malabo Convention with the distinction being that the former is legally binding.<sup>100</sup>

#### **4.2. TDF Mechanism/Tools**

Upon creation of an African single market by the Agreement Establishing the African Continental Free Trade Area (AEAFCTA), TDF has been partly institutionalized into the African data protection legal framework by implication.<sup>101</sup> In spite of this implied infusion, except a harmonized mechanism is created to ease TDF in Africa, the idea of a single market is seriously endangered. Taking into account the nuances of African economic and socio-political circumstances and with the necessary modification, African governments can adopt the EU model to ease TDF without compromising data subjects’ rights and freedoms.

##### *1.1.1 Standard Contractual Clauses (SCCs)*

Under the GDPR, in the event of absence of adequacy decision in favour of a country, a controller/processor is duty bound to provide safeguards for protection of data subjects’ rights

---

<sup>98</sup> B. Zeller ‘Uniformity of Laws: A Reality or just a Myth?’ (2008) 1(3) International Journal of Private Law, 231.

<sup>99</sup> Anal Assioua, ‘Data Privacy. How a Lack of Uniformity is Detrimental to Progress’ (2019) < <https://www.humanrightsadvocates.org/wp-content/uploads/2019/03/Assioua-Data-Privacy.pdf>> accessed 17 July 2022.

<sup>100</sup> Some African Countries have also ratified the Convention 108, to wit: Burkina Faso, Cape Verde, Mauritius, Morocco, Senegal and Tunisia < <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=108>> accessed 14 July 2022.

<sup>101</sup> Emmanuel Salami, ‘Implementing the AFCTTA Agreement: A Case for the Harmonization of Data Protection Law in Africa’ (2022) 66(2) Journal of African Law, 281-291.

before TDF can take place. One of the approved safeguards is the execution of contracts embedded with standard contractual clauses (SCCs) approved by the European Commission.<sup>102</sup> SCCs are prescribed special guidelines that regulate flow of personal data between EU and non-EU countries/entities. SCCs are not only intrinsically manageable and available, the Court of Justice of European Union has ruled on them as ‘appropriate safeguards’ mechanism under the EU data protection legal system in *Schrems II case*.<sup>103</sup>

The African Union (AU) can take a cue from Europe by devising bespoke standard data protection clauses to safeguard the rights and freedoms of African citizens and/or residents during TDF within the context of African trade and sundry transactions. This will ensure uniformity of safeguards in the event of uncertainty of the level of data protection measures in the recipient-country.

### *1.1.2 Binding Corporate Rules (BCRs)*

BCR – another European TDF-device was introduced as an acceptable tool for compliance with the strict EU adequacy requirements. A BCR is an internal but binding corporate policy setting out the enforceable rules applicable to intra-company transfer of personal data with international substances.<sup>104</sup> Within the EU, BCRs are officially and generally accepted by the supervisory authorities as adequate legal mechanism for TDF within and outside the region.

The African committee of DPAs can borrow a leaf from this as it will be helpful to agree on a template for BCRs especially for African business with parent bodies in other jurisdictions. Ultimately, BCRs constitute more flexible tools that will enable African entities scale the European adequacy hurdle and ease TDF into the EEA region without violating the applicable laws.<sup>105</sup>

### *1.1.3 Improved Cooperation between African DPAs*

---

<sup>102</sup> General Data Protection Regulation, article 46 (2)(d).

<sup>103</sup> Case C-311/18, Data Protection Commission v Facebook Ireland Limited, Maxmilian Schrems, see also Laura Bradford et al, ‘Standard Contractual Clauses for Cross- Border Transfers of Health Data After Schrems II’ (2002) 8(1) Journal of Law and Bioscience, 1-36. They are also referred to as ‘model contracts clauses’, ‘standard data protection clauses or ‘safe- harbor’.

<sup>104</sup> Oliver Proust, ‘Binding Corporate Rules: A Global Solution for International Data Transfers’ (2012) 2(1) International Data Privacy Law, 35.

<sup>105</sup> Philip Pees, ‘Binding Corporate Rules: A Simpler Clear Version?’ (2007) 23 Computer Law and Report, 352-356.

In every data protection ecosystem, data protection authorities (DPAs) play a significant role in ensuring compliance and efficiency of designed mechanisms. The Malabo Convention mandates African DPAs to cooperate with DPAs elsewhere towards international development of data protection framework.<sup>106</sup> Greenleaf et al however argue that, as a consequence of this provision an African DPAs coalition<sup>107</sup> – Network of African Data Protection Authorities (NADPA) - was created in 2016 even though an earlier body of African DPAs had been created since 2007.<sup>108</sup> For proper impact in the regulation of TDF, it is desirable for the coalition of existing DPAs in Africa to agree on and develop uniform framework for safe TDF in Africa based on international standards. Admittedly, not all member states of the AU have functional DPAs as a result of ‘lack of political will, competing priorities and financial constraints,’<sup>109</sup> yet the existing and operational ones can collectively regulate TDF in Africa as done in the EU.<sup>110</sup>

#### *1.1.4 Regional Adoption of right to privacy as a fundamental right*

There’s no gainsaying that the right to privacy has no place in the African Charter even though researchers have argued that the right can be inferred from other provisions of the international instrument.<sup>111</sup>

---

<sup>106</sup> African Union (AU) Convention on Cyber Security and Personal Data Protection, article 12(2) (m).

<sup>107</sup> See Graham Greenleaf and Bertil Cottier, ‘International and Regional Commitment in African Data Privacy Laws: A Comparative Analysis (2022) 44 Computer Law & Security Review, 12.

<sup>108</sup> The ‘Association francophone des autorités de protection des données personnelles’ (AFAPDP) was created in Montreal in September 2007. See < <https://www.afapdp.org/>> accessed 16 July 2022.

<sup>109</sup> Mercy King’Ori et al ‘A look into DPA strategies in the African Continent’ (2022) < <https://fpf.org/blog/fpf-report-a-look-into-dpa-strategies-in-the-african-continent/>> accessed 12 July 2022.

<sup>110</sup> It is however instructive to note that in March 2022, Smart Africa (an initiative of African Heads of State) signed a MoU with NADPA for the enhancement of collaboration between DPAs for data protection regulation on the continent. See <https://www.businessghana.com/site/news/business/259069/Smart-Africa-NADPA-Sign-MOU-on-enforcement-of-data-protection-laws>> accessed 11 July 2022.

<sup>111</sup> Mavendzenge argues that other fundamental rights provided under the African Charter impose obligations on government to respect and protect right to privacy. See Justice Alfred Mavedzenge ‘The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance’ (2020) 12(3) African Journal of Legal Studies, 360-390; Ayalew interestingly argues that reliance can be placed on the flexibility clause in the African Charter in the regional courts to invoke relative provisions to enforce the right to privacy, see Yohannes E. Ayalew, ‘Untrodden Paths Towards the Right to Privacy in the Digital Era under African Human Rights Law’ (2022) 2(1) International Data Privacy Law, 160; see also Kinfe M. Yilma et al ‘Safeguards of Right to Privacy in Ethiopia: A Critique of laws and Practices (2013) 26 Journal of Ethiopia Law, 106 and Avani Singh et al. ‘The Privacy Awakening: The Urgent Need to Humanize the Right in Africa’ (2019) 3 African Human Right Yearbook, 202.

Whether by amendment of the African Charter as suggested by Heyns and Viljoen<sup>112</sup> or by elevation through a resolution of the ACHRPR,<sup>113</sup> right to privacy must be expressly provided and guaranteed under the regional human rights instruments in Africa. On the insufficiency and danger in the current states of right to privacy on the continent, Singh and Power succinctly capture the unsavoury situation thus:

“While key efforts to fully introduce the right to privacy in the region have taken place, full recognition of the right is yet to occur. The rapid advancements in, and use of, ICTs -- domestically, regionally, and globally warrants an urgent and holistic response to the right to privacy in Africa. In the absence of the recognition of the right to privacy and data protection as a fundamental right in the African Charter, and its concomitant status as a lodestar for RECs, the current piecemeal and un-harmonised approach limits the ability of all people on the continent to realise their privacy rights or seek vindication for violations from regional bodies and courts. This must be urgently remedied.”<sup>114</sup>

#### 4. CONCLUSION

Africa’s lack of binding regional framework and her divergent national laws on data protection will continue to haunt and hurt TDF on the continent. Conversely, international movement of personal data within and outside Africa has become inherently illegal or made unnecessarily expensive by regulatory bottlenecks in some cases. While it is conceded that regulation of TDF remains a global problem, Africa’s struggles with the concept remain hydra headed. The existing regional conventions that sparingly touch on TDF are either unenforceable or unhelpful towards provision of clarity or uniformity of purpose. The various national laws are also at variance on provision of safeguards or essential TDF mechanisms.

From the foregoing, a meaningful approach must necessarily commence with a workable Africa-wide framework that does not only define TDF from an African perspective but one that also sets

---

<sup>112</sup> Christof Heyns and Frans Viljoen, ‘An Overview of International Human Rights Protection in Africa’ (1999)15 South African Journal of Human Rights, 421.

<sup>113</sup> This is contained in a recommendation by Privacy International at the 62<sup>nd</sup> session of the African Commission on Human and People’s Right (ACHR) at Novakchott, Mauritania in April 2018.

<sup>114</sup> Avani Singh and Michael Power, ‘The Privacy Awakening: The Urgent Need to Harmonize the Right to Privacy in Africa’ (2019) 3 African Human Yearbook, 202-220.

out the workable and realistic enforcement procedure given our current economic and socio-political peculiarities. In this paper I have discussed how the divergence of data protection and data localization laws have continued to hamper economic benefits of TDF in Africa. Even though the paper downplays blind reliance on European framework, the paper suggests African solutions to Africa's problems in that regard while taking cue from the European experience having been in the field since 1970.