Journal of African Law, 66, 2 (2022), 281–291 © The Author(s), 2022. Published by Cambridge University Press on behalf of SOAS University of London.
doi:10.1017/S0021855322000110 First published online 6 May 2022

Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa

Emmanuel Salami*
Faculty of Law, University of Lapland, Rovaniemi, Finland
Emmanuel.Salami@ulapland.fi

Abstract

The Agreement Establishing the African Continental Free Trade Area (AEAfCFTA) is a revolutionary treaty of the African Union (AU) which creates an African single market to guarantee the free movement of persons, capital, goods and services. The AEAfCFTA is geared towards enabling seamless trade among African countries. The single market relies heavily on the processing of the personal data of persons resident within and outside the AU, thereby necessitating an effective data protection regime. However, the data protection regime across Africa is fragmented, with each country either having a distinct data protection framework or none at all. This lack of a uniform continental framework threatens to clog the wheels of the African Continental Free Trade Area (AfCFTA), because by demanding compliance with the various data protection laws across Africa, free trade will be inhibited, the very problem the AEAfCFTA seeks to remediate. These concerns are considered and applicable solutions are proposed to ensure the successful implementation of the AfCFTA.

Keywords

AEAfCFTA, AfCFTA, data protection, Africa, privacy, free trade

INTRODUCTION

The implementation of a single market through the Agreement Establishing the African Continental Free Trade Area (AEAfCFTA) is arguably one of the more important projects of the African Union (AU). A single market is one "in which the free movement of goods, persons, services and capital is ensured and where citizens, individuals and businesses can seamlessly conduct business under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence".[1]

---

* Emmanuel Salami is a doctoral candidate in Information Technology, Data Protection, and Intellectual Property Law at the Faculty of Law, University of Lapland, Finland.

1 European Commission, Commission Staff Working Document "A digital single market strategy for Europe: Analysis and evidence. Accompanying the document: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A digital

One clear objective of single markets is the removal of inhibitions likely to limit trade; however, concerns such as a lack of trust in the single market, or certain sectors of it, may arise. For instance, some market participants may be deterred from trading in a single market when fundamental human rights (including the right to data protection) are not adequately protected. The subsistence of a single market hinges largely on the free flow and processing of large volumes of (personal) data. Therefore, where personal data is not lawfully processed, some market participants may be dissuaded from partaking in the single market.

The journey towards the realization of the African Continental Free Trade Area (AfCFTA) can be traced back to the year 2012, when the Assembly of Heads of State and Government of the AU accepted the establishment of a pan-African free trade area by 2017.[2] As will be considered, the aim of the AfCFTA is the development of a single market for the promotion of the free movement of goods, persons and services;[3] the AfCFTA is particularly significant because of its status as the largest free trade area in the world.[4] The negotiations preceding the adoption of the AEAfCFTA were long and arduous before it entered into force on 30 May 2019 in the 24 countries that ratified it.[5] At the time of writing, 54 out of the 55 member states of the AU have signed the AEAfCFTA, with Eritrea being the only country yet to supply its signature.[6]

The importance of the AEAfCFTA cannot be overstated, especially because of its potential to eliminate the barriers to intra-African trade and boost the African economy in the process. The AEAfCFTA harmonizes (at least theoretically) the different sectors of the African economy, which will play a role in the implementation of the single market; these harmonizations eliminate

---

contd
single market strategy for Europe", COM(2015) 192 final, Brussels, 6.5.2015, SWD(2015) 100 final at 3. See also R Simo "The African Continental Free Trade Area in a decaying multilateral trading system: Questioning the relevance of the enabling clause" (2019) *SSRN* at 1, available at: <https://ssrn.com/abstract=3501539> (last accessed 11 August 2021).

2 African Union "Assembly of the Union: Eighteenth ordinary session" (January 2012), available at: <https://au.int/sites/default/files/decisions/9649-assembly_au_dec_391_-_415_xviii_e.pdf> (last accessed 14 August 2021).

3 For further reading on the aims and objectives of the AfCFTA, see C Onyejekwe and E Ekhator "AfCFTA and lex mercatoria: Reconceptualising international trade law in Africa" (2021) 47/1 *Commonwealth Law Bulletin* 95.

4 The World Bank "The African Continental Free Trade Area" (2020), available at: <https://www.worldbank.org/en/topic/trade/publication/the-african-continental-free-trade-area> (last accessed 14 August 2021).

5 The Trade Law Centre (Tralac) "African Continental Free Trade Area (AfCFTA) legal texts and policy documents" (2021), available at: <https://www.tralac.org/resources/our-resources/6730-continental-free-trade-area-cfta.html#legal-texts> (last accessed 17 March 2022).

6 "About AfCFTA" (2021), available at: <https://www.africancfta.org/aboutus> (last accessed 14 August 2021).

https://doi.org/10.1017/S0021855322000110 Published online by Cambridge University Press

divergent national (economic) policies which can hinder the development of the single market. Curiously, it would appear that the continent's fragmented data protection framework has not been taken into consideration in the harmonization of the African market. This poses a threat to the flourishing of the single market, because diverse national compliance requirements diminish the possibility of achieving its "barrierless" element. This article highlights how some provisions of the AEAfCFTA conflict with some (national) data protection provisions and the possible single market inhibitions that may arise therefrom. Possible resolutions to these issues will also be considered. The existing framework for data protection law in Africa will be discussed, and will be followed by an examination of specific provisions of the AEAfCFTA which might impact on (national) data protection laws. The legal framework that has been adopted for the harmonization of data protection law in the European Union (EU) single market will also be considered.

A BRIEF OVERVIEW OF THE REGULATION OF DATA PROTECTION LAW IN AFRICA

Even though attempts at a continental harmonization of data protection law in Africa have been made, its regulation remains fragmented and falls under the national laws of respective AU member states. The African Union Convention on Cyber Security and Personal Data Protection (the Convention)[7] is the most tangible evidence of a continental attempt to harmonize data protection law across the continent; it acknowledges the necessity of creating uniform commitments for the protection of personal data across the continent.[8] However, the convention is yet to be ratified by a significant number of AU member states,[9] thereby making its coming into force a legal impossibility.[10] For the purpose of this article, the legal framework of

7 African Union Convention on Cyber Security and Personal Data Protection (27 July 2014) EX.CL/846(XXV).

8 See the Preamble of the Convention.

9 At the time of writing, only eight out of a total of 55 AU countries have ratified the AU convention. Thirteen other countries (Benin, Chad, Comoros, Congo-Brazzaville, Guinea-Bissau, Mauritania, Mozambique, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia and Zambia) have signed but not ratified it. "List of Countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection" (18 July 2020), available at: <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> (last accessed 17 March 2022). See also G Greenleaf and B Cottier "Comparing African data privacy laws: International, African and regional commitments" (2020) *University of New South Wales Law Research Series*, available at: <https://ssrn.com/abstract=3582478> (last accessed 28 October 2020).

10 Art 36 of the Convention makes its ratification by fifteen AU member states a condition of its coming into force.

https://doi.org/10.1017/S0021855322000110 Published online by Cambridge University Press

African data protection can be categorized into the continental, regional and national approaches.

The continental approach manifests in the form of the Convention, yet to come into force. There are also some regional data protection instruments, including the Economic Community of West African States' Supplementary Act on Personal Data Protection within ECOWAS (2010),[11] and the Southern African Development Community's Model Act on Data Protection (2013),[12] but their actual impact on members can at best be described as persuasive.[13] From the perspective of a national approach and at the time of writing, 32 African countries have enacted national data protection laws; five countries have pending bills before their respective legislative institutions, while 18 countries are yet to enact any data protection regulatory instruments.[14] Based on the above information, it would appear that a national approach to data protection regulation is currently favoured across the continent, which means that the requirements for data protection compliance varies across the African continent.

THE AEAFCFTA V (NATIONAL) DATA PROTECTION LAWS: IDENTIFYING POTENTIAL SINGLE MARKET BARRIERS

The AEAfCFTA creates frameworks for the harmonization of potential barriers to the realization of the single market among AU member states. This article argues that some provisions of the AEAfCFTA might suffer implementation setbacks as a result of the diverging approaches in national data protection law among individual AU member states. To consider some relevant examples: firstly, AEAfCFTA, part IV, art 15 provides that subject to non-arbitrariness or unjustified discrimination, states shall be authorized, inter alia, to adopt or enforce measures necessary for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts", so long as such measures are not inconsistent with the AEAfCFTA provisions on the free movement of services.[15] This sole reference to privacy in the AEAfCFTA pertains only to trade in services and does not extend to the free movement of persons,

11 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (16 February 2010), available at: <statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf> (last accessed 17 March 2022).

12 Available at: <https://www.dataguidance.com/legal-research/data-protection-southern-african-development-community-sadc-model-law-0> (last accessed 5 April 2022).

13 For other relevant regional data protection laws, see Greenleaf and Cottier "Comparing", above at note 9 at 20. For further reading, see A Makulilo (ed) *African Data Privacy Laws* (2016, Springer).

14 See Greenleaf and Cottier "Comparing", above at note 9 at 3.

15 This clause necessarily includes not just privacy law but also data protection law. This is because the "processing and dissemination of personal data" falls within the purview of data protection law. See for example the Data Protection Act of Kenya 2019, sec 2.

https://doi.org/10.1017/S0021855322000110 Published online by Cambridge University Press

capital and goods; it therefore appears that the AEAfCFTA considers only the former privacy considerations as necessary. Alternatively, this provision can be interpreted as reserving legislative sovereignty over the privacy of goods, persons and capital to state parties. This approach poses a potential hinderance to the free movement not only of services but also of persons, capital and goods, owing to state parties' authorization to draft their own privacy and data protection laws. To take advantage of the single market and carry out services within it, businesses and other relevant stakeholders will necessarily have to process personal data across multiple member state jurisdictions within the AU. Since the AEAfCFTA allows AU member states to adopt their own measures for data protection when it involves the movement of services, service providers will be required to comply with the different data protection instruments in the various jurisdictions of the AU member states they operate in. However, national laws must not be inconsistent with the provisions of the AEAfCFTA – it is yet to be seen how this inconsistency will be avoided. While this provision against inconsistency is laudable, it could be better achieved through a harmonized continental data protection framework. Even though the provision of AEAfCFTA, part IV, art 15 applies expressly to trade in services, the scenario above is expected to apply to trade in persons, capital and goods in practice.

Secondly, AEAfCFTA, part V, art 18 mandates state parties to accord each other (and be able to negotiate) favourable preferences on a reciprocal basis. From a data protection perspective, this implies that state parties, subject to conditions which include reciprocity, can negotiate compliance on various points of divergence in their national data protection laws. This may result in the fragmentation of data protection law compliance across the continent, with different state parties negotiating "favorable preferences" among themselves,[16] which will potentially distort the single market and will also contradict the AfCFTA's objective to create a single market and deepen the economic integration of the continent, as stipulated in AEAfCFTA, part II, art 3. If the AfCFTA's aim of creating a single market is to be achieved, the market fragmentation that will arise from its approach to intra-African data protection compliance, as demonstrated by this provision, ought to be addressed.

Furthermore, art 16(4) of the Protocol on Rules and Procedures on the Settlement of Disputes in the AEAfCFTA provides, inter alia, that in the settlement of disputes, confidential information that is provided to the dispute settlement panel[17] shall not be disclosed without formal authorization from the source providing the information. This means that for state parties to formally authorize the disclosure of confidential information which might include personal data, they will have to comply with the applicable law

16 See AEAfCFTA, part V, art 18(2).

17 Id, art 9 (Protocol on Rules and Procedures on the Settlement of Disputes) establishes a dispute settlement panel tasked with the resolution of disputes arising out of the AEAfCFTA.

(including data protection law) governing its disclosure. Since the governance of data protection law is different across the continent, the conditions that have to be met to authorize the disclosure of confidential information will also necessarily vary. It will be interesting to see how dispute resolution mechanisms which are inherent in national data protection legislation(s) will be balanced against the AEAfCFTA's dispute resolution framework.[18] This might extend the time frame for authorizing data disclosures across various member states, which might result in potential delays to the decision-making process of the panel. Furthermore, there is the possibility that parties might take advantage of divergences in the governance of data protection law across the continent to delay and frustrate the efforts of the panel to settle disputes.

Another potential single market barrier might be found in AEAfCFTA, part IV, art 8, which provides that each state party may introduce new regulations on services and service suppliers within its territory in order to meet national policy objectives insofar as such regulations do not impair any rights and obligations arising under the Protocol. This clause notwithstanding, state parties are empowered to adopt their own data protection instruments, which might affect the free movement of services anticipated under the AEAfCFTA. Beyond the provision of services, this clause might also be relevant for countries lacking laws which regulate the processing of the personal data of AU residents by businesses located outside the AU, and in such cases, countries can possibly rely on this provision to draft detailed data protection laws.[19] Interestingly, this provision also signals the intention of the AU to adopt a synchronization of African data protection laws, rather than their harmonization.[20] In other words, it would appear that the AU chose to allow state parties to retain their legislative sovereignty to make data protection laws as they deem fit, insofar as such laws remain compliant with the objectives of the single market. This regulatory approach apparently places less burden on the legislative framework of the AU and may also have reduced the chance of debates and disagreements that may have stifled the initial adoption of the AEAfCFTA. However, the problem might only have been deferred, as state

18 For example, see the dispute resolution mechanism established under sec 4(2) of the Nigerian Data Protection Regulation 2019, which varies from other national legislations.

19 From an African perspective, this kind of business model is to be expected in a single market. In the EU, in *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság*, a Slovakian entity was transacting business in Hungary even though it had no physical office there. The Court of Justice of the European Union held that the fact that the Slovakian business had a website aimed at Hungarians, and other factors that showed intent to target them, was sufficient justification to indicate that it was targeting Hungarians. See *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] C-230/14.

20 Synchronization in this context requires that state parties align their respective laws in a manner geared towards the facilitation of the objectives of the single market; harmonization requires that state parties of the AU will have a single law for the regulation of data protection law across the continent.

parties still have to meet and agree on the applicability of relevant data protection laws; this places the responsibility on state parties to agree on favourable clauses among themselves, which, I argue, will result in the fragmentation of the single market and the eventual contradiction of its objectives. The harmonization of the African single market through the adoption of a uniform African data protection law will therefore be more favourable to the establishment of a truly single market across the continent.

Divergence in national approaches to data protection governance might be seen, for instance, where the processing of personal data by entities located outside the AU is regulated in some countries and unregulated in others. Another instance includes where data localization requirements differ from one jurisdiction to another; for example, while the Nigerian Data Protection Regulation (NDPR) contains no data localization requirements,[21] the Data Protection Act of Kenya provides that "the Cabinet Secretary may prescribe … certain nature of processing that shall only be effected through a server or a data centre located in Kenya".[22] This means that entities will have to adopt different approaches to data governance in Nigeria and Kenya. Within the context of the AEAfCFTA, this might potentially hinder the single market because, ordinarily, entities ought to have the freedom to store their data within the market subject to their business needs and convenience, and aimed towards the free movement of persons, capital, goods and services within the AU. Therefore, a divergence of this nature will only create restrictions which will be inimical to the single market objectives of the AfCFTA.

Since entry into the single market will not be limited only to entities domiciled in the AU, the divergence in data protection laws across the continent might particularly restrain free entry for such entities due to conflicting compliance requirements, and this will invariably fetter the freedom of trade which the AfCFTA seeks to establish. Another consequence of regulatory fragmentation is that business entities might find it difficult to pull (personal) data together for achieving a single purpose because each country has different compliance requirements. For instance, section 53 of the Data Protection Act of Kenya provides, inter alia, that further processing of personal data shall be compatible with the purpose of collection if the data is used solely for research purposes and is not published in an identifiable form. Section 39 of the same act also provides, inter alia, that personal data intended for research purposes may be retained even after the purpose for its collection has been satisfied. The data localization possibilities under the Data Protection Act of Kenya would also be a significant consideration for these processing activities. On the other hand, in South Africa the Protection of Personal Information Act (POPIA)[23] provides a more detailed framework for the

21 See the Nigerian Data Protection Regulation.

22 Data Protection Act of Kenya, sec 50.

23 Act No 4 of 2013, vol 581, no 37067. POPIA came partly into force on 1 July 2020 and became fully applicable on 30 June 2021. For further readings on POPIA, see

regulation of personal data for research purposes; section 14(2) provides that "personal information"[24] may be retained for research purposes even after the initial purpose of its collection has been satisfied so long as appropriate safeguards have been taken against the records being used for any other purpose, and section 27(1)(d) provides that the restrictions on processing sensitive personal data[25] do not apply where the processing is for research purposes.[26] Section 35(1)(d) also permits the processing of the personal data of children for research purposes, while section 37(2)(e) provides that the regulator may authorize the processing of personal data in circumstances where such processing activity would ordinarily be unlawful. Based on these provisions, South Africa has a very expansive framework for personal data processing for research purposes.[27] In Nigeria, section 2(1)(a)(i) of the NDPR, on the other hand, permits, inter alia, further processing of personal data for research purposes. In these three AfCFTA member states, then, businesses will have to meet different standards to be able to conduct research with personal data; the nature of personal data that will be available will also vary, and the possibility of using similar categories of data for research across these jurisdictions stands to be potentially onerous: the options to use personal data for research purposes in South Africa are quite expansive while the possibilities for similar activities in Kenya are more restrictive and might be inhibited by the country's requirement for data localization. This situation will not make intra-African trade any easier and could frustrate the free movement of persons, capital, goods and services sought by the AfCFTA. Furthermore, the process of drafting and signing data protection agreements across the continent will pose another challenge, as businesses will be required to enter into distinct and specially drafted data protection agreements, with divergent obligations subject to the applicable national laws. This will make contracting onerous, particularly from a data protection perspective, while also creating a hurdle which will fetter the single market and make it less attractive.

Another possible consequence of the application of divergent national data protection laws is the fact that some countries will adopt stricter laws than others. In such cases, one can expect that data controllers and processors will be more inclined to comply with stricter data protection laws, as this will consequently help them comply with weaker data protection laws as a

---

contd
Werksmans Attorneys "An introduction to POPIA" (May 2020), available at: <https://www.werksmans.com/legal-updates-and-opinions/popia-a-guide-to-the-protection-of-personal-information-act-of-south-africa/> (last accessed 16 May 2021).

24 POPIA refers to personal data as personal information. See the definition of personal information in POPIA, sec 1.

25 On the definition of personal data and sensitive personal data within the Act, see id, secs 1 and 26.

26 Id, sec 32(5)(b) also authorizes the processing of health-related data for health purposes.

27 This article makes no comment on the necessity or effects of these provisions on the protection of personal data or the right to data protection as this is not its objective.

matter of course. In such a situation, data controllers and processors might also be inclined to engage in "forum shopping", which might even influence their business' choice of countries of domicile if this helps them avoid a requirement of compliance with stricter data protection laws. The implication of this will likely be inconsistent rights to data protection, with data subjects resident in countries with stricter data protection laws enjoying a better level of protection than others. The fragmentation of African data protection law, with some state parties affording data subjects a higher standard of protection than others, means that persons trading across the single market will be subject to varying levels of protection as they carry out transactions across the continent, which, depending on the nature of the business, might be a deterrent for some companies.[28]

TOWARDS A TRULY UNHINDERED AFRICAN SINGLE MARKET

The concerns pertaining to the potential inhibition of the single market because of divergent national approaches to the regulation of data protection law can be resolved if the continent adopts a uniform regulatory approach. The effect of the initial fragmentation of data protection law within the EU provides some context to what can be expected from a data protection-induced fragmentation of the African single market.

The EU framework on data protection law was previously governed by the Data Protection Directive (DPD),[29] which established the data protection objectives sought in the EU while allowing member states to determine how best to achieve those objectives.[30] This legislative approach meant that different EU member states devised their own means of achieving the goals sought by the DPD, thereby resulting in the fragmentation of the framework. The effect of this fragmentation on the EU single market included inconsistent data protection requirements for businesses across the EU, the non-regulation of data

28 For instance, a business requiring client confidentiality (e.g. cloud computing companies storing client data) might be reluctant to transact business in countries where there are no data protection laws for reasons which include the possibility of unlawful data requisition by national governments. Conversely, such companies might find such countries attractive for business because of little or no need for data protection compliance. Either way, the rights to data protection of data subjects are bound to be violated.

29 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281, 23.11.1995, at 31.

30 A directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. See European Union "Regulation, Directives and other Acts", available at: <https://europa.eu/european-union/law/legal-acts_en#:~:text=A%20%22directive%22%20is%20a%20legislative,how%20to%20reach%20these%20goals> (last accessed 15 November 2020).

https://doi.org/10.1017/S0021855322000110 Published online by Cambridge University Press

controllers or processors domiciled outside the EU, etc.[31] As a result of these shortcomings, the General Data Protection Regulation (GDPR)[32] was conceived as a regulatory instrument aimed at creating a uniform regime for the governance of data protection law in the EU. The GDPR sought to (and does) achieve this through three steps: the establishment of a (more) coherent legal framework that enhances legal certainty in the development of the digital economy in the EU;[33] ensuring the free flow of personal data within the EU to support the functioning digital single market;[34] and the establishment of uniformity in the regulation of data protection law across the EU. By adopting this approach, fair competition is achieved because both European and non-European businesses[35] are bound by the same rules, irrespective of where in the EU they engage in business.[36]

It is reasonable to expect that the African single market will be confronted with challenges similar to those that faced the EU single market before the GDPR came into force.[37] To prevent this, I would recommend that a uniform African data protection law be adopted to ensure a consistent application of data protection law within the jurisdiction of AU member states. So far, the Convention is the closest attempt at a uniform continental approach to the regulation of African data protection law. Though the Convention might be lacking in fundamental provisions which are necessary for the effective regulation of data protection,[38] it is a decent start towards achieving continental standardization that facilitates the foundational growth of the African single market. A preferrable and more progressive approach would be amending the Convention, thereby plugging the gaps I have identified. The adoption of a uniform regulatory approach to data protection across the African continent means that companies will be spared the cost and resources (including their capital, workforce, time, etc.) which would otherwise have been invested

31 European Commission "A digital single market strategy for Europe", above at note 1 at 46.

32 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016.

33 Id, recitals 7 and 13.

34 Id, recital 13.

35 Some specific rules may necessarily differ between EU and non-EU businesses. An example of this can be found in id, art 27 on the appointment of representatives by entities offering goods to EU residents or monitoring EU residents from outside the EU.

36 V Reding "The EU data protection regulation: Promoting technological innovation and safeguarding citizens' rights" (4 March 2014), available at: <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_175> (last accessed 19 November 2020).

37 European Commission "A digital single market strategy for Europe", above at note 1.

38 At the time of writing, one of the major shortcomings of the Convention which makes it less suitable as an appropriate law for data protection regulation across the continent is the fact that it does not regulate the processing of personal data by data controllers not located within the AU. In other words, the Convention does not contain a provision similar to GDPR, art 3(2).

towards complying with the divergent requirements of the various national data protection laws of AU state parties.

The importance of data protection law to global trade cannot be overemphasized. As earlier highlighted with the example of data localization laws,[39] data protection restrictions can delegitimize ordinarily justifiable trade relationships. This possibility, and other trade restrictions not related to data protection, ought to be eliminated in a truly single market. However, without a uniform approach to the regulation of data protection law across the continent, this might just end up being another lofty and unimplementable African aspiration.

CONCLUSION

The rationale justifying the adoption of a uniform African approach to data protection law has been discussed in this article, and the consequences of the fragmentation of data protection in the AU single market has also been considered. AU member states have shown their determination to open up intra-African trade for economic growth; it is hoped that this resolve can also be transformed into a force that ensures the effective eradication of potential fetters in the workings of the single market. Attempts at synchronizing, rather than harmonizing, data protection rules across the continent will hinder the single market objectives of the AfCFTA, and the possibility of divergent data protection laws, limiting the realization of free intra-African trade, opposes the freedom of trade which the AfCFTA seeks to establish. Finally, the challenges that were faced in the EU single market will hopefully serve as a lesson to the AU and its state parties, and the identified pitfalls will be avoided. While the AEAfCFTA is a great step forward for Africa, it is hoped that further amendments will reconsider the establishment of a uniform framework for African data protection law geared (among other things) towards the elimination of fragmentation in the single market.

CONFLICTS OF INTEREST

None

39 Data Protection Act of Kenya, sec 50.

https://doi.org/10.1017/S0021855322000110 Published online by Cambridge University Press