THE MALABO ROADMAP

Approaches to promote data protection and data governance in Africa

mozilla

THE MALABO ROADMAP:

Approaches to promote data protection and data governance in Africa

September 2022

Prepared for the Mozilla Africa Mradi programme by ALT Advisory.

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS

AfCFTA	African Continental Free Trade Area
AU	African Union
AUC	African Union Commission
AUCSEG	African Union Cybersecurity Expert Group
Budapest Convention	Budapest Convention on Cybercrime, 2001
DPA	Data Protection Authority
DPAs	Data Protection Authorities
EU	European Union
GDPR	General Data Protection Regulation of the European Union 2016/679
Lomé Declaration	Lomé Declaration on Cybersecurity and the Fight Against Cybercrime
Malabo Convention or the Convention	African Union Convention on Cyber Security and Personal Data Protection, 2014
NADPA/RAPDP	Network of African Data Protection Authorities
NAWC	Network of Women in Cybersecurity
PoA	Plan of Action
RECs	Regional Economic Communities
RIA	Research ICT Africa
SADC	Southern African Development Community
Smart Africa	The Smart Africa Alliance
STC	Specialised Technical Committee (of the African Union)
US	United States of America

EXECUTIVE SUMMARY

1. This document outlines a Roadmap to advance legal frameworks for data protection and cybercrime in Africa. It aims to guide a process of public discussion on bringing into force the African Union (AU) Convention on Cyber Security and Personal Data Protection, 2014 (**the Malabo Convention or the Convention**) as a continental framework to advance data protection and privacy in the region.
2. As connectivity continues to improve across the continent, it is time for the implementation of a common continental instrument that ensures protection for digital rights, including data protection and cybersecurity.
3. The African Union adopted the Malabo Convention in 2014 to establish such a framework for the continent, by mandating states to develop legal frameworks for the protection of personal data, the promotion of cybersecurity, the combating of cybercrime, and standards for e-commerce.
4. The Malabo Convention will come into force when fifteen AU member states submit articles of ratification. While the slow pace of ratification has been cause for concern, as of March 2022 the number of ratifying states had increased to thirteen, bringing the prospect of its coming into force within reach.
5. This Roadmap has been developed to assesses the desirability and feasibility of the entry into force of the Malabo Convention, and identifies complementary interventions or strategies that can augment the regulation of cybercrimes and data protection in Africa.

The case for prioritising the Malabo Convention

6. As of July 2022, 22 African countries still do not have data protection laws in place. Those with data protection laws continue to face significant challenges to implementation, enforcement, low levels of transparency, and a lack of institutional independence.
7. A strong case for prioritising the Malabo Convention is that it offers a cohesive continent-wide framework to advance and harmonise data protection policies in African societies, especially in light of the general trend towards regional and continental data protection frameworks. If brought into force and properly implemented, the Malabo Convention could yield advantages for human rights, economic development, good governance and policy coherence on the continent. It could promote better protections for key digital rights in Africa, especially data protection and the right to privacy, and create the necessary conditions for Africa's economic development in the information age. Most notably, if properly implemented, the Malabo Convention could be crucial to achieving the AU's vision of a single market in Africa, through the African Continent Free Trade Area (**AfCFTA**) Agreement.

Addressing concerns about the Malabo Convention

8. Although the Malabo Convention may be a feasible path to better digital rights protections, possible weaknesses and gaps in the Convention must also be assessed. A key criticism seen in the literature and from civil society is that the Convention is both over-inclusive and under-inclusive in its scope: it seeks to unify broad issues of cybercrime, cybersecurity, data protection, and e-commerce into one overarching framework, while simultaneously lacking important details, such as lacking provision for monitoring and enforcement mechanisms. In addition, while the Convention mandates protections for basic rights such as freedom of expression and the right to privacy within states' cybersecurity policies, these safeguards could benefit from further development.

Identifying the 'Malabo opportunity'

9. There is now momentum both for the Malabo Convention and broader data protection policies on the continent. This presents a clear policy window for establishing a harmonised framework dedicated to cybersecurity and data governance. A strong case can thus be made that bringing the Malabo Convention into force will allow the continent to gain ground within the digital economy and on digital rights, while also setting a standard for coherent and harmonised policy on these issues for the Africa continent.

10. While the Convention is not yet in force, it is close to the fifteen ratifications needed to bring it into operation, after four additional states submitted their instruments of ratification for the Convention to the AU in 2021 and 2022. Thus, the pursuit of ratification and implementation of the Malabo Convention is both an achievable goal and worthy priority for policymakers on the continent, especially as global trends sway in favour of regional or continental data protection frameworks.

Next steps in the Malabo Roadmap

11. This Roadmap analyses three 'next steps' in pursuit of improved data governance in Africa: (1) it assesses the desirability of, and likely pathways to, ratification and implementation of the Malabo Convention; (2) it identifies important policy interventions to complement the Malabo Convention and address any gaps; and (3) it proposes an awareness-raising strategy to bring together important stakeholders to develop and advance these proposals. It calls on like-minded partners and potential allies to join the conversation and bolster these efforts by bringing their own perspectives to bear on the strategies identified and to mobilise their networks and resources to advance efforts to improve data governance in Africa.

Pathways to ratification

12. Noting that two more member states must submit articles of ratification to the AU to bring the Malabo Convention into force, the Roadmap proposes certain factors to be considered as local and regional civil society bodies and data protection advocates assess whether a particular AU member state might ratify the Convention. These factors are: the state's existing position as signatory to the Malabo Convention; their domestic momentum on data protection and cybersecurity policy; their regional influence as a data protection actor; and their favourable process for ratification.

Important complementary policy interventions

13. The Roadmap emphasises the importance of working with existing complementary efforts focused on cybercrime and data governance on the continent, including those of the Smart Africa Alliance and the AU Data Policy Framework, to harmonise policy processes and address gaps in the Convention.
14. The Roadmap also identifies the need to pursue implementation guidelines and a Plan of Action (**PoA**) for the domestication of the Malabo Convention in member states, to bridge the gap between the continental framework and the implementation of domestic legislation. This requires engagement with the AU Commission and Regional Economic Communities (**RECs**). These additional efforts can be referred to as the "**Malabo Plus**" approach.
15. The Roadmap also acknowledges the possible value of the AU Commission developing a new Convention to eventually replace the Malabo Convention, which would seek to comprehensively address any shortcomings and anachronisms in the Malabo Convention as adopted. This policy option may be dubbed "**Malabo 2.0**". Given the risk that an entirely new Convention could face long delays in drafting, adopting and ratification, and given the apparent achievability of operationalising the current Malabo Convention, the Roadmap argues that this option is best pursued as *complementary* to the "Malabo Plus" approach, rather than as an alternative.

Awareness-raising interventions

16. Building on an assessment of the prospects of the Convention, and the need for complementary policy interventions, the Roadmap proposes a series of engagements and awareness-raising efforts that will involve multi-stakeholder communities, including the African Union Commission (**AUC**), domestic Data Protection Authorities (**DPAs**), government stakeholders, and civil society actors. These efforts will focus in particular on communities in five target states to amplify the discussion on bringing the Convention into force and to engage on pursuing complementary policy interventions to augment the Convention.

17. The awareness-raising activities will focus on stakeholder engagement and public dialogue to stimulate discussion on the propositions:

    17.1 The Malabo Convention is an *achievable policy goal*;

    17.2 The Malabo Convention is an opportunity to *improve data protection and digital rights*;

    17.3 The Malabo Convention is an opportunity for *African development*, especially in line with the vision of a single market in Africa in terms of the AfCFTA;

    17.4 The Malabo Convention would *strengthen African sovereignty*, especially by helping to shift the power dynamics between global technology giants and African societies.

    17.5 The Malabo Convention can, and should, be complemented by additional policy interventions, such as Implementation Guidelines and a Plan of Action for domestic implementation, that would mitigate against some of its weaknesses and augment its efficacy.

    Data governance can be improved in Africa by passing the Malabo Convention in the short-term and then initiating efforts to develop a new, complementary regional instrument – Malabo 2.0 – to further respond to data governance challenges that are not fully addressed by the Malabo Convention.

ENDS.

A. INTRODUCTION

Overview and aims of the Malabo Roadmap

1. This document outlines a roadmap to advance legal frameworks for data protection and cybercrime in Africa, including through analysing prospects to bring into force the African Union (**AU**) *Convention on Cyber Security and Personal Data Protection, 2014*[1] (**Malabo Convention** or **Convention**) as a continental framework and lodestar on data protection and privacy in the region.
2. The primary aim of this Roadmap is to inform continental discussions among a diverse set of stakeholders on the advancement of international law instruments regulating cybercrimes and data protection in Africa. It also aims to determine whether making progress towards the entry into force of the Malabo Convention is feasible and desirable, as well as to identify additional instruments or interventions that can augment the regulation of cybercrimes and data protection in Africa. The Roadmap outlines the ratification status of the Malabo Convention and schools of thought on the regional governance of these issues, and defines a case for future action to advance data protection frameworks on the continent, both through and in addition to, the Malabo Convention.
3. Crucially, it is clear that this will involve building multi-stakeholder communities to work towards these objectives that include (1) the African Union Commission (**AUC**); (2) regional networks of Data Protection Authorities (**DPAs**), and DPAs themselves; (3) government stakeholders such as Ministries of Foreign Affairs; and (4) civil society organisations and actors.

B. THE CASE FOR THE MALABO CONVENTION

Overview of the Malabo Convention and data protection in Africa

4. The Malabo Convention was initially drafted in 2011 to establish a "credible framework for cybersecurity in Africa through [the] organisation of electronic transactions, protection of personal data, promotion of cyber security, e-governance, and combating cybercrime." The adoption of the Malabo Convention was postponed several times after earlier versions of the document faced criticism from the private sector, civil society organisations, and advocates for digital rights and freedoms.[2] The draft Malabo Convention was reviewed by an AU-convened meeting of experts in May 2014, before being redrafted and finally adopted in June 2014. Since then, AU member states have been slow to ratify the Malabo Convention, although as of 25 March 2022, thirteen states have ratified it, bringing it close to the fifteen ratifications needed to bring it into operation.[3]
5. The Malabo Convention aims to create a harmonised legal framework on data protection and cybersecurity in Africa. It does so by mandating that every member state should establish domestic laws on the relevant policy areas that meet various criteria detailed in the Convention.[4] These include electronic transactions, data protection, and cybersecurity and cybercrime.

Electronic transactions

6. While the Malabo Convention's provisions on electronic transactions are less relevant for the purposes of this Roadmap, in brief, the Convention provides a set of harmonised standards and rules on various forms of e-commerce, including electronic advertising, the status of electronic contracts, and payment security for electronic transactions.[5]

---

1 African Union Convention on Cyber Security and Personal Data Protection, 2014, accessible here.
2 Access Now, 'Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa', 2016, accessible here, at 1.
3 African Union, 'Status List: List of countries which have signed, ratified/acceded to the Malabo Convention', 25 March 2022, accessible here.
4 Malabo Convention above n 1 at Article 36.
5 *Id* at Articles 3-7.

Data protection

7. The Malabo Convention mandates every state to establish a data protection framework, "aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and to punish any violation of privacy without prejudice to the principle of the free flow of information."[6] This framework is to be monitored and enforced by a national data protection authority (**DPA**) with administrative independence, and a duty to ensure that the processing of personal data is duly regulated.[7] Each state's framework for the processing of personal information should align with core data protection principles, such as consent, lawfulness, confidentiality, and transparency,[8] with various rights conferred on every person concerning the protection of their data.[9]

Cybersecurity and cybercrime

8. The Malabo Convention mandates every member state to develop a national cybersecurity policy and strategy,[10] and to establish various institutions and procedures to identify and respond to cybersecurity incidents, promote cybersecurity principles, and ensure international cooperation.[11] In terms of cybercrime, the Convention directs member states to adopt domestic legislative and regulatory measures to criminalise "acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process, and the underlying network infrastructure."[12]
9. In doing so, the Convention outlines and briefly defines various acts which should be legislated as criminal offences in each state's domestic measures, such as attacks on computer systems, fraudulent access to or interception of computer data, and various content-related offences.[13] The content related offences include using a computer system to produce, disseminate, or possess child pornography through a computer system;[14] give a minor access to pornography;[15] create, download, or disseminate writing, messages, or visual or other media of "ideas or theories of racist or xenophobic nature";[16] threaten to commit a criminal offence against a person or people for the reason that they belong to a group "distinguished by race, colour, descent, national or ethnic origin or religion";[17] and insult a person or people for the reason that they belong to a group "distinguished by race, colour, descent, national or ethnic origin or religion or political belief".[18]
10. Noting that these provisions, in particular, may have implications for freedom of expression, Article 25(3) of the Convention provides that in establishing cybersecurity frameworks states "will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights such as freedom of expression, the right to privacy, and the right to a fair hearing, among others."[19]

---

6 *Id* at Article 8(1).
7 *Id* at Article 11.
8 *Id* at Article 13.
9 *Id* at Articles 16-19.
10 *Id* at Article 24.
11 *Id* at Articles 26-28.
12 *Id* at Article 25(1).
13 *Id* at Article 28.
14 *Id* at Article 28(3)(1)(a)-(c).
15 *Id* at Article 28(3)(1)(d).
16 *Id* Article 28(3)(1)(e).
17 *Id* at Article 28(3)(1)(f).
18 *Id* at Article 28(3)(1)(g).
19 *Id* at Article 25(3).

Prevailing approaches to continental data protection frameworks

11. In the years since the passage of the *General Data Protection Regulation*[20] (**GDPR**) of the European Union (**EU**), the prevailing view in many policy circles has been toward regional frameworks on data protection. In the global context, the GDPR has been crucial in advancing and harmonising data protection principles in the world's biggest single market and establishing a benchmark for data protection regulation internationally. By dint of its place within the EU, one of the world's biggest economies, the GDPR also presents an imperative for other countries and international industries to establish equivalent data protection measures. In the African context, the case for a continental framework for data protection includes meeting these imperatives, but it should also be viewed in the context of the domestic and continental demand for domestic data protection regimes in Africa, which would further enable regional trade and economic development.

12. Despite what has been criticised as slow progress, there have been significant advances within the region in recent years. As of July 2022, 33 countries in Africa had enacted fully dedicated data protection legislation — a significant improvement in the past decade. However, 22 African countries did not have data protection laws in place. Many of those countries with data protection laws continue to face significant hurdles to implementation, low levels of transparency, and a lack of institutional independence.[21]

13. Commonly cited economic, political, and rights-based benefits to a more structured, regional approach to data governance include:

    13.1 Facilitating trust, consistent policymaking, and fostering competition and cooperation in digital trade among African states.[22]

    13.2 Aligning domestic data protection policies to foster collaboration, learning, and the development of regional best practices in data protection, thus lowering the costs and other barriers to implementation observed at a national level.[23]

    13.3 Creating a framework for domestic and regional momentum and advocacy to speed up the development and implementation of domestic data protection policies among states that are lagging.

14. Cross-border data flows are a significant consideration in the economic case for regional data protection frameworks. Data localisation — policies and laws to restrict the flow of data across borders — may in certain contexts uphold important data protection principles, but cumbersome or overbroad restrictions on the transfer of data across national borders come at a severe cost to economic development, job creation, and global competitiveness.[24] Notably, several policy analyses have observed a trend towards data localisation and nationalisation in African jurisdictions.[25] A regional or continental data protection framework offers a harmonised approach to enabling cross-border data transfers between member states, while providing standards and safeguards for data protection principles.[26]

15. While global data protection policy trends lean towards regional frameworks, this approach is not without criticism. In observing the early years of implementation of the GDPR since it entered force in 2018, the most common criticisms centre on cost, complexity, and implementation. EU authorities continue to grapple with the harmonisation of member states' data protection laws, and have, in particular, struggled to deal effectively with crossborder cases — a key mechanism to align data protection principles with crossborder data flows.[27] A study on the implementation of the GDPR in ten countries found that most of the national adaptations are still incomplete and may

---

20 European Union, General Data Protection Regulation 2016/679, accessible here.
21 Paradigm Initiative, *Data Protection Authorities in Africa (DPAS) Report*, 2021, accessible here.
22 Centre for the Study of the Economies of Africa, 'Strengthening Data Governance In Africa', 2021 at 16.
23 *Id*.
24 Atabey, 'The Potential Economic Empowering Role of Cross-border Data Flows for Data Protection in Africa' in Sampath Tregenna (eds), *Digital Sovereignty: African Perspectives*, University of Johannesburg, Johannesburg, 2022 at 24.
25 Kugler, 'The Impact of data localisation laws on trade in Africa' *Policy Brief 8* The Mandela Institute, School of Law, University of the Witwatersrand, 2021 at 2.
26 Kugler *Id* at 6-7.
27 European Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition — two years of application of the General Data Protection Regulation', COM 2020 264, June 2020 at 5.

not fully conform with the GDPR.[28] The significant cost of GDPR compliance has also been noted.[29] However, it should be noted that a key argument *for* regional data protection frameworks is that, by creating harmonised policy across a range of markets, a regional approach seeks ultimately to simplify compliance and reduce costs.

Arguments in favour of the entry into force of the Malabo Convention

16. From an African perspective, the most likely cases *in favour* of advancing the Malabo Convention can be separated into several, interconnected themes: a rights-based case, an economic case, a case for policy coherence and harmonisation, and a pragmatic case for advancing other policy priorities through ratification of the Malabo Convention.

Protection and advancement of rights

17. The Malabo Convention can be a strategic pathway to domesticating data protection and cybersecurity laws in Africa. Despite notable progress in the past decade, it is concerning that as many as 22 African states do not have any data protection law in place, and many of those states with a domestic data protection framework are lagging in implementation, resourcing, and necessary reforms and amendments. If brought into operation, the Malabo Convention would serve as a roadmap to advancing and harmonising data protection policy across the continent, which could both promote and advance fundamental rights for people in Africa, and advance states' obligations in terms of regional and international human rights law.

Policy coherence and momentum

18. The Malabo Convention would facilitate vital policy coherence in the region by creating a set of policy goals for all AU members to work towards and by creating clear standards and norms for those laws and their implementation. Additionally, by creating regional alignment in these laws, the Convention could enable better and faster implementation at a domestic level by fostering collaboration, mutual learning, and the development of regional best practices. An early example of this has already occurred with the emergence of the Network of African Data Protection Authorities (**NADPA/RAPDP**), a continent-wide body established in September 2016.[30]

Economic development and implementation of the AfCFTA

19. The Malabo Convention would likely facilitate regional data flows between African countries by ensuring appropriate mechanisms for data protection.[31] This is seen as an important factor in promoting trade, economic development, and job creation.[32]
20. More specifically, the Malabo Convention's harmonisation of data protection and cybersecurity policy could also be an enabling step in achieving the AU's primary economic priority: the vision to create a single market in Africa through the African Continental Free Trade Area (**AfCFTA**), which was brought into operation in 2019 and is now subject to negotiations among the member states.[33] By its nature, the single market, which would enable the free flow of people, goods, and capital throughout Africa, requires extensive processing of personal data across borders. The lack of a coherent continent-wide data protection framework has been flagged as a major obstacle to the implementation of the AfCFTA[34].

---

28 McCullagh, Tambou and Bourton (eds), *National Adaptations of the GDPR*, Collection Open Access Book, Blogdroiteuropeen, Luxembourg, 2019.
29 Chen, Frey and Presidente, 'Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally', The Oxford Martin Working Paper Series on Technological and Economic Change (Working Paper No. 2022-1), January 2022.
30 Network of African Data Protection Authorities (NADPA/RAPDP) website, accessible here.
31 Kugler above n 25 at 7.
32 Atabey above n 24 at 24.
33 African Continental Free Trade Area (AfCFTA), About, accessible here.
34 See Salami 'Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa' *Journal of African Law*, 1-11 (2022), doi:10.1017/S0021855322000110.

Advancing other regional policy priorities

21. Pragmatically, ratification of the Malabo Convention could play a role in advancing other regional policy priorities. These include AfCFTA, as explored above, and the AU's Agenda 2063, a 50-year development plan for Africa which has adopted the development of cybersecurity as one of its flagship programmes.[35] A final pragmatic point in favour of advancing the Malabo Convention: *it is an achievable policy goal*. Allowing for any shortcomings of the Convention as an instrument, the fact that there is a feasible path to bringing it into operation should be counted in its favour.

Arguments against the entry into force of the Malabo Convention

22. Some of the key cases *against* advancing the Malabo Convention can be grouped into the following themes: its overall content and scope, its implications for digital rights, the challenges in the ratification process, and certain perceptions that data protection policies reflect Western or European influence on Africa.

Overall content and scope

23. Critics have raised concerns about the content and scope of the Convention.

    23.1 First, that it is overbroad: the decision to parcel together such a wide range of information policy concerns into the Convention has resulted in both legal complexity and political complexity by requiring that ratifying states are willing to endorse a wide range of policy issues all at once. In tying human rights issues, commercial issues, and criminal law into the same instrument, the Convention has also been criticised for a diminished focus on data protection.[36]

    23.2 Second, the Convention has been criticised for various provisions which are considered vague, inconsistent, or archaic: the Convention makes various references, for example, to 'personal data', 'electronic data', 'physical data', and 'computerized data', but does not define all these terms or distinguish clearly between them,[37] and leaves several other important terms and processes either loosely defined or undefined.[38]

24. Additionally, the Convention has been criticised for certain important omissions: for example, the Convention does not provide for data breach notifications or privacy impact assessments,[39] or mechanisms to monitor or support the implementation of the Convention at a regional level.[40]

25. The cybercrime provisions of the Convention have also raised concern as appearing, in some instances, to be at odds with provisions of the pre-existing *Budapest Convention on Cybercrime, 2001*[41] (**Budapest Convention**) to which several AU member states are already parties,[42] although these inconsistencies appear to be resolvable.

Digital and information rights

26. While the framing and stated objectives of the Malabo Convention affirm its purpose as an instrument for the protection and promotion of human rights,[43] and amendments to earlier drafts of the Convention sought specifically to address rights-based concerns, the Convention does face criticism for inconsistent protections for digital and information rights.

---

35 African Union, 'Agenda 2063: The Africa We Want', accessible here.
36 Abdulrauf and Fombad, 'The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?' *Journal of Media Law*, 2016, doi: 10.1080/17577632.2016.1183283 at 23-4.
37 *Id* at 24-5.
38 Council of Europe, 'Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime' (November 2016), accessible here, at 5.
39 Abdulrauf and Fombad above n 36 at 25.
40 *Id* at 31.
41 Budapest Convention on Cybercrime, 2001, accessible here.
42 Council of Europe above n 38 at 5-7.
43 Malabo Convention above n 1 at Preamble.

27. The Convention enjoins member states to ensure that their cybersecurity legislation is in line with domestic and internationally recognised human rights protections and should not infringe on basic rights such as freedom of expression and the right to privacy.[44] However, given the regional trend towards cybersecurity and cybercrime laws which are often overbroad, open to abuse, and which serve to criminalise legitimate online speech and dissent,[45] it has been argued that this does not constitute a sufficiently robust safeguard.

28. While the majority of offences provided for in the Convention's cybercrimes provisions conform to the existing framework established in the Budapest Convention, certain drafting in the Malabo Convention leans toward the potential for over-criminalisation,[46] such as the 'insult' provisions in Article 29.[47] The procedural powers granted to state authorities in the Convention also tend to exclude sufficient safeguards and conditions that will limit the risk of abuse.[48]

Political inertia

29. Most analyses of the Malabo Convention note the slow process of ratification since its adoption in 2014. There may be a lingering view that the Convention suffers from political inertia, and that the overall objectives of the Convention are better achieved through other national, regional, and continental approaches. However, recent momentum around the Convention, with four countries submitting instruments of ratification to the AU in 2021 and 2022, has brought the number of ratifying states to thirteen[49] — suggesting that the "inertia" case against the Convention may no longer hold.

The influence of European policy

30. While it is not clear how widely this view is held, certain analyses have argued that the Malabo Convention — and many national-level approaches to data protection and cyber policy in Africa — reflect external pressure and internal tendencies in African societies to import or approximate European data protection regimes,[50] whether or not they are fit for purpose. It is also correctly argued that African laws and policies on privacy and data protection must be shaped by local norms and values. It is important to note, though, that the idea that notions of privacy and data protection are incompatible with predominant cultural values in African societies has largely been debunked and that African-centric conceptions of privacy can and should be advanced.[51]

31. Importantly, an argument that data protection approaches in Africa, both at a national level and in the Malabo Convention itself, reflect Western hegemony may be redundant: the more compelling case is that a harmonised continent framework in Africa, whatever its inspiration, will *strengthen* Africa's position in the global domain — both in relation to powerful economies like the United States (**US**), Europe, and China, and in relation to dominant technology companies in the West and Asia.[52] It has been argued that the policy inertia which has stalled ratification and implementation of the Malabo Convention has left many African countries in holding patterns "that are essentially set by companies originating from China, the US, and the EU."[53]

---

44 *Id* at Article 25.
45 Symantec 'Cyber Crime and Cyber Security Trends in Africa', 2016, accessible here at 56.
46 Council of Europe above n 38 at 48-75.
47 Article 29(1)(g) of the Malabo Convention provides: "State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to [i]nsult, through a computer system, persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, or religion or political opinion, if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics."
48 Council of Europe above n 38 at 5.
49 See above n 3.
50 See Bryant, 'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights' *Stanford Technology Law Review*, Vol. 24:2, 2021 at 417.
51 See, for example, Makulilo, '"One size fits all": Does Europe impose its data protection regime on Africa?' *Datenschutz und Datensicherheit* 7, 2013.
52 See stakeholder remarks in Center for Global Development, 'Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development' CDG Brief, 2021, accessible here.
53 Ayodele, 'Big Tech: Not-so-Simple Politics' in Gehl Sampath and Tregenna (eds), Digital Sovereignty: African Perspectives, University of Johannesburg, Johannesburg, 2022 at 103.

Weighing the arguments for and against the Malabo Convention

32. While the Malabo Convention is not an ideal instrument and lacks some contemporary nuance, pursuing ratification and implementation of the Convention presents a real pathway to better protections for digital and information rights in Africa — albeit a challenging one. The Convention is a tangible framework to advance data protection and cybersecurity laws and institutions across Africa — and with recent ratifications from several AU member states, the Convention is close to the threshold of entering into force. Therefore, even at a pragmatic level, while the Convention may be imperfect, its entry into force is, at least, achievable in the near-term.
33. On balance, this suggests that the pursuit of ratification and implementation of the Malabo Convention, among other things, is a worthwhile priority for policymakers and digital rights advocates. Recognising some of the problems identified in the text of the Convention itself and the likely hurdles to implementation, an effort to advance the Malabo Convention should be joined with a range of other strategies. These are explored in the Conclusion and Recommendations sections below.
34. In recognition of the value of harmonising other ongoing processes, this Roadmap turns briefly to consider related processes at the regional and international levels which any effort to advance the Malabo Convention should seek to complement.

Other processes underway

The Budapest Convention on Cyber Crime

35. The 2001 Budapest Convention[54] is the only binding international instrument on cybercrime, and serves as a useful guideline for countries developing cybercrime legislation. The Convention was the first international effort to provide guidelines for countries to develop their national legislation and to establish a framework for international cooperation, which is crucial for the investigation and prosecution of trans-national cybercrime.
36. Five African states are already party to the Budapest Convention: Cabo Verde, Ghana, Mauritius, Morocco, and Senegal.[55] All but Morocco have also ratified the Malabo Convention. Any state may be a party to the Budapest Convention once it has developed a law that domesticates the key provisions of the Budapest Convention. The following African states have been invited to accede to the Budapest Convention as a result of their recent legislative developments: Benin, Burkina Faso, Nigeria, Niger, South Africa, and Tunisia.
37. For alignment, it is argued that while the Malabo Convention does not go as far as the Budapest Convention in creating an actionable framework for international harmonisation and cooperation on cybercrime, there is value in treating the two instruments as complementary and building on AU member states' political commitment to develop cybercrime policy through the Budapest Convention *and* the Malabo Convention.[56]

The Smart Africa Alliance

38. Launched in 2013, the Smart Africa Alliance (**Smart Africa**) is an alliance of 32 African countries, international organisations, and global private sector actors tasked with advancing Africa's digital agenda. Smart Africa brings together heads of state who seek to accelerate the digitalisation of the continent and create a common market, and has already undertaken several strategic initiatives to advance data protection and cybersecurity policy and implementation across Africa. These include:

54 Budapest Convention above n 41.
55 Council of Europe, 'The Budapest Convention and its Protocols', accessible here.
56 Council of Europe above n 38 at 5.

38.1 Capacity-building and development of data protection authorities: In March 2022, Smart Africa and the NADPA/RAPDP signed a memorandum of understanding to support authorities' enforcement and harmonisation of personal data protection laws.57

38.2 *Developing a Pan-African framework on data protection and privacy*: After forming a Data Protection Working Group in support of states' efforts to develop data protection strategies and policies, in March 2021 Smart Africa announced a project to develop a Pan-African framework on data protection and privacy,[58] which it aims to put into operation within three years. This initiative appears to be aimed at identifying the harmonisation challenges between different national and regional frameworks and developing strategies to address policy conflicts, improve the implementation and enforcement of data protection frameworks, and improve the capacity of DPAs.

38.3 *Developing a cybersecurity blueprint for Africa*: Similarly, in March 2022 Smart Africa announced a project to develop a cybersecurity blueprint for Africa, seeking to harmonise cybersecurity frameworks on the continent and develop institutions and processes to enhance regional cooperation on cybercrime.[59]

The AU Data Policy Framework

39. In addition to Smart Africa's Pan-African Framework and blueprint, the African Union Commission, supported by Research ICT Africa (**RIA**), has developed the *AU Data Policy Framework for Africa*.[60] The Framework sets out "a common vision, principles, strategic priorities and key recommendations to guide African Union Member States in developing their national data systems and capabilities to effectively derive value from data that is being generated by citizens, government entities and industries."[61]

40. The Framework follows a recommendation in the *AU Digital Transformation Strategy for Africa*[62] and "builds on a range of existing initiatives and frameworks including the Policy and Regulatory Initiative for Digital Africa (**PRIDA**), the Programme for Infrastructure Development in Africa (**PIDA**), the African Continental Free Trade Area (**AfCFTA**), the African Union Financial Institutions (**AUFIs**), the Single African Air Transport Market (**SAATM**), the Free Movement of Persons (**FMP**), and the Malabo Convention, to support the development of a Digital Single Market (**DSM**), as part of the integration priorities of the African Union. Data governance is recognised as an essential cross-cutting theme to support the digital ecosystem."[63]

57 RAPDP, 'Smart Africa et NADPA/RAPDP ont signé un protocole d'accord pour faire progresser l'application et l'harmonisation des lois sur la protection des données personnelles en Afrique', 13 March 2022, accessible here.
58 Smart Africa, 'Request for proposals for the recruitment of a consultancy firm to draft a Pan-African framework on data protection and privacy' 24 March 2021, accessible here.
59 Smart Africa, 'Recruitment of a consultancy firm to develop a continental blueprint for the Cybersecurity Project for Africa' 11 March 2022, accessible here.
60 African Union, 'AU Data Policy Framework', 2022, accessible here at 3.
61 *Id*.
62 Digital Transformation Strategy for Africa (2020-2030), accessible here.
63 African Union, above n 60. at 3.

C. PATHS TO RATIFICATION

41. In order to come into force, the Malabo Convention must be ratified by at least fifteen member states.[64] At the time of writing, thirteen member states have ratified the Convention, which comes into operation 30 days after the fifteenth instrument of ratification is submitted.[65] To the extent that entry into force of the Malabo Convention should be a priority, this section assesses the current ratification status of the Convention and possible pathways for the Convention to reach the threshold of fifteen ratifying states.

Current ratifications and signatories

42. To date, the Convention has been ratified by **thirteen** AU member states:[66] Angola, Cabo Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia. A total of fourteen states have signed the Convention, **nine** of which have not yet ratified: Benin, Chad, Comoros, Gambia, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome and Principe, and Tunisia. As a result, two more states need to ratify the Convention to bring it into force.

Identifying states amenable to ratifying the Malabo Convention

43. As local and regional civil society bodies and data protection advocates consider the bringing into force of the Malabo Convention, they may consider several characteristics of AU member states that would affect the prospects of ratification within those states, including whether states have:

    43.1 Engaged favourability with the Convention, for example through signatory status;

    43.2 Indicated responsiveness to ratifying AU instruments in general;

    43.3 Domestic laws which enable ratification;

    43.4 Developed data protection frameworks and institutions;

    43.5 Domestic civil society and public sectors which are receptive or favourable towards localised advocacy and partnerships; and

    43.6 Regional influence in policymaking.

D. CONCLUSION

44. Pursuing ratification of the Malabo Convention presents a pathway to better protections for digital rights in Africa, albeit a challenging one. Foremost, the Convention represents a clear strategic framework to advance data protection and cybersecurity laws and institutions across Africa, which intervention is sorely needed. There is a feasible pathway to the Convention entering into force, by being ratified by at least two more member states. The recent issuing of the *Lomé Declaration on Cybersecurity and the Fight Against Cybercrime* (**Lomé Declaration**) by several AU member states, which renews the call for states to ratify and implement the Convention,[67] suggests that the Convention continues to be a live issue.

45. However, there are weaknesses to the Malabo Convention, which must be anticipated and addressed. These include that the Convention is both over-inclusive, by bundling data protection, cybercrime, cybersecurity, and e-commerce into one legal framework, and under-inclusive, by omitting important definitions and processes and lacking provision for mechanisms to monitor and ensure compliance and enforcement. The Convention, while providing that states' cybersecurity legislation should not infringe on basic rights such as freedom of expression and the right to privacy,[68]

64 Article 36 of the Malabo Convention above n 1.
65 *Id.*
66 African Union above n 3
67 The Lomé Declaration on Cybersecurity and the Fight against Cybercrime, 2022, accessible here.
68 Article 25 of the Malabo Convention above n 1.

does not provide full and robust safeguards against rights infringements. Considering these factors, advancement of the Malabo Convention is likely to be most feasible, and most effective, if joined with complementary efforts, outlined below. These complementary efforts are especially important in ensuring proper implementation of the Malabo Convention, if or when it enters into force.

46. Therefore, the following sections outline a set of policy interventions that could enhance the Malabo Convention — dubbed "Malabo Plus" — and a proposed advocacy and awareness plan to build support and momentum towards these goals.

Recommendations to augment the Malabo Convention

47. Any effort to pursue ratification of the Malabo Convention should also address the shortcomings in the Convention, and lay the groundwork for further efforts to promote effective implementation of the Convention. Several recommended avenues may be considered.

Further development of the Convention through the preparation of implementation guidelines and a Plan of Action (PoA)

48. If or when the Convention is brought into operation, pathways for the AUC to develop its interpretation and implementation through guidelines should be pursued. Such interventions, which could build on existing and emerging practices within the AUC,[69] could seek to address gaps in the Convention and engage with emerging issues in data protection and cybersecurity, such as (1) appropriate protections for human rights in the use of artificial intelligence; (2) protections for privacy, freedom of expression, and related rights in the context of mass surveillance capacities of member states, foreign state actors, and private actors; (3) recommended measures to ensure appropriate resourcing, implementation, and institutionalisation of domestic data protection frameworks; and (4) the establishment of regional agencies or bodies, through RECs, to monitor and support implementation and enforcement of the Convention.
49. Practically, this may include:
    49.1 Developing implementation guidelines and a Plan of Action (**PoA**) for the domestication of the Malabo Convention in the Member States.
    49.2 Engaging with the AUC and RECs to harmonise existing regional frameworks and develop regionalised implementation guidelines and PoAs.

Development of a model African data protection law

50. In light of the significant delays in the passage of the Malabo Convention, the development of a model African data protection law may support states in implementing the relevant provisions of the Convention once it enters into force. Such an effort may build on existing model laws: for example, the Southern African Development Community (**SADC**) issued a model data protection law in 2013,[70] and the Commonwealth, whose membership includes **nineteen** African states, developed a model bill on the protection of personal information in 2017.[71] (The initiative undertaken by Smart Africa to develop a Pan-African framework for data protection is a significant opportunity in this regard, and any effort to advance the Malabo Convention should seek to align with this.)

69 See for example The Internet Society & The African Union Commission, *Personal Data Protection Guidelines for Africa*, 2018, accessible here.
70 SADC, 'Data Protection: Southern African Development Community Model Law', 2013, accessible here.
71 Commonwealth Secretariat, 'Model Bill on the Protection of Personal Information', 2017, accessible here.

Consideration of a future Convention to succeed Malabo

51. In the long-term, there is possible value for the AU Commission to seek development of a new Convention eventually to succeed the Malabo Convention, which would aim to address any shortcomings and anachronisms in the original instrument. However, given the possible delays and obstacles that could be expected in drafting, adopting, and operationalising an entirely new Convention, there are notable risks to abandoning the current Convention now that it is on the cusp of coming into force. Rather, the policy objectives of the AU and its member states might be best served if this option is approached as a complementary step alongside the feasible step of operationalising the existing Malabo Convention.

Continued support for data protection authorities in Africa

52. Acknowledging that most African DPAs are in a nascent stage, further work to develop the institutional capacities of specific DPAs may assist with advancing the implementation of the Malabo Convention once it enters into force, while aligning and supporting the efforts of the RAPDP.

Awareness-raising activities

53. The final section of this Roadmap outlines an approach to stimulate public discussion on bringing the Malabo Convention into force, and pursuing the various interventions to augment the Convention, outlined in the previous section.
54. Previous assessments of obstacles to ratification within AU member states have noted that, except where member states have declared a specific reason for a delay in ratification, the likely factors include a lack of participation in negotiations, limited awareness of the convention or treaty, and inadequate mechanisms at national and regional levels to ensure ratification.[72] In the light of this, the Roadmap proposes stakeholder engagements that address *limited awareness* of the Malabo Convention and promote active discussion on the issue of *a lack of participation or ownership* in the development of the Convention.

Awareness-raising interventions

55. It is proposed that awareness-raising interventions be undertaken that build partnerships with civic actors, including civil society organisations (**CSOs**) and academics, and state-aligned bodies such as DPAs, and that facilitate multilateral engagement with member states and the AU Specialised Technical Committees (**STCs**) on Justice and Legal Affairs and on Communications and Information Technology, and regional institutions.
56. STCs are thematic Committees within the AU comprising member states' ministers and senior officials responsible for particular policy sectors.[73] STCs work with AUC departments to ensure harmonisation of AU projects and programmes as well as coordination with the Regional Economic Communities (**RECs**). These STCs meet at the ministerial and expert levels every two years.[74]
57. Discussions on the Malabo Convention should include engaging with the STC on Justice and Legal Affairs, whose area of competence includes following up on ratification of AU treaties, and the STC on Communication and Information Communications Technology (**ICTs**), which is responsible for developing frameworks for ICT policy and regulatory harmonisation in Africa.

---

72 Anywar, 'Consultant's Report of the Study on the Development of Strategy to Guide the Promotion of the Ratification of the Revised African Convention on the Conservation of Nature and Natural Resources (i.e. the MAPUTO CONVENTION)' African Union Commission, 2016, accessible here.

73 African Union, 'Specialised Technical Committees,' accessible here. STCs were established under Article 14 of the AU Constitutive Act.

74 African Union Assembly/AU/Dec.365(XVII), accessible here.

58. It should further be noted that, in January 2018, the 32nd Ordinary Session of the Executive Council endorsed a decision of the Specialised Technical Committee on ICTs to create an Africa Cyber Security Collaboration and Coordination Committee to advise the AUC on Cyber strategies and to implement the Cyber Security flagship project of Agenda 2063.[75] As a result, the African Union Cybersecurity Expert Group (**AUCSEG**) held its first meeting in Addis Ababa, Ethiopia in December 2019.[76] One of the AUCSEG's tasks is to propose solutions to facilitate the ratification and domestication of the Malabo Convention into national laws, and engagement with the AUCSEG should therefore also be a priority.

Stimulating discussion on the Malabo Convention

59. In conclusion, it is proposed that collective efforts to advance data governance in Africa begin by facilitating robust public discussion on the following propositions:

    59.1 **Malabo is *achievable*:** The long and slow process of drafting and ratification of the Malabo Convention, and regional and international instruments in general, often make it a low priority for public officials, policymakers, and civil society actors. The recent momentum behind the Convention suggests that there is a real opportunity to bring it into operation. The apparent achievability of the Convention is also likely an important consideration for stakeholders who are wary of certain provisions in the Convention, but who recognise *some* benefits of bringing it into operation.

    59.2 **Malabo is an opportunity for *data protection and digital rights*:** Despite its shortcomings, the Malabo Convention can be seen as a crucial step in addressing serious gaps and delays in policy and implementation on data protection across Africa.

    59.3 **Malabo is an opportunity for *African development*:** Advancing data protection policy across Africa is not only important to protect and advance human rights, but a vital step toward economic development, trade, and job creation. In particular, the Malabo Convention can be seen as complementary to the vision of a single market in Africa in terms of the AfCFTA.

    59.4 **Malabo strengthens *African sovereignty*:** Despite some scepticism that the Malabo Convention or prevailing national data protection laws in Africa reflect a Western policy hegemony, a truly harmonised, robust continental data protection framework can strengthen Africa's place in the world by: (1) ensuring a coherent response to frameworks like the GDPR, with geopolitical and trade benefits; and (2) shifting the power dynamics between global technology giants and African societies. A fully implemented Malabo Convention could enhance protections for African citizens, both in relation to their own governments, and in relation to local and global technology providers.

    59.5 **Malabo can, and should, be complemented by additional policy interventions**: Implementation Guidelines and a Plan of Action for domestic implementation could mitigate against some of the Convention's weaknesses and augment its efficacy.

    59.6 **Malabo can be complemented by a separate, future instrument**: Data governance can be improved in Africa by passing the Malabo Convention in the short-term and then initiating efforts to develop a new, complementary regional instrument — Malabo 2.0 — to further respond to data governance challenges that are not fully addressed by the Malabo Convention.

ENDS.

75 African Union 'African Union Cybersecurity Expert Group holds its first inaugural meeting,' 2019, accessible here.
76 *Id*.

USEFUL RESOURCES

Abdulrauf and Fombad, 'The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?' *Journal of Media Law*, 2016, doi: 10.1080/17577632.2016.1183283.

Access Now, 'Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa', 2016.

African Union, 'Study on the Procedures for Ratification of Treaties in Member States, Harmonization of Ratification Procedures and Measures to Speed Up the Ratification of OAU/AU Treaties', 2008, MinJustice/Legal/4 Rev 2.

African Union, 'Digital Transformation Strategy for Africa (2020-2030)', 2022.

African Union, 'AU Data Policy Framework', 2022.

Anywar, 'Consultant's Report of the Study on the Development of Strategy to Guide the Promotion of the Ratification of the Revised African Convention on the Conservation of Nature and Natural Resources (i.e. the MAPUTO CONVENTION)' African Union Commission, 2016.

Atabey, 'The Potential Economic Empowering Role of Cross-border Data Flows for Data Protection in Africa' in Sampath Tregenna (eds) *Digital Sovereignty: African Perspectives* (University of Johannesburg, Johannesburg 2022).

Ayodele, 'Big Tech: Not-so-Simple Politics' in Gehl Sampath and Tregenna (eds) *Digital Sovereignty: African Perspectives* (University of Johannesburg, Johannesburg 2022).

Bryant, 'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights' *Stanford Technology Law Review*, Vol. 24:2, 2021.

Center for Global Development, 'Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development' CDG Brief, 2021.

Centre for the Study of the Economies of Africa, 'Strengthening Data Governance In Africa', 2021.

Chen, Frey, and Presidente, 'Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally' *The Oxford Martin Working Paper Series on Technological and Economic Change* (Working Paper No. 2022-1, January 2022).

Council of Europe, 'Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime' (November 2016).

ALT Advisory, Data Protection Africa, https://dataprotection.africa.

European Commission, 'Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation' (COM (2020) 264 final, June 2020).

Kugler, 'The Impact of data localisation laws on trade in Africa' Policy Brief 8 The Mandela Institute, School of Law, University of the Witwatersrand, 2021.

Makulilo, '"One size fits all": Does Europe impose its data protection regime on Africa?' *Datenschutz und Datensicherheit* 7, 2013.

Malawu, 'Ratification of African Union Treaties by Member States: Law, Policy and Practice', *Melbourne Journal of International Law,* Vol 13, 2012.

McCullagh, Tambou, and Bourton (eds), *National Adaptations of the GDPR*, Collection Open Access Book, Blogdroiteuropeen, Luxembourg, 2019.

Paradigm Initiative, *Data Protection Authorities in Africa (DPAS) Report*, 2021.

Summary Report of the Meeting of Experts on the Review of the OAU/AU Treaties, AU Doc OAUAU Treaties/Exp-PRC/Rpt. (I) Rev.I, 2004.

The Internet Society and the African Union Commission, *Personal Data Protection Guidelines for Africa,* 2018.

Salami, 'Implementing the AfCFTA Agreement: A Case for the Harmonization of Data Protection Law in Africa' *Journal of African Law,* 1-11 (2022), doi:10.1017/S0021855322000110.

Symantec, 'Cyber Crime and Cyber Security Trends in Africa', 2016.