AfriSIG 2024: Multistakeholder consultation on implementing the African Continental Free Trade Area (AfCFTA) digital protocol in compliance with the African Union Data Policy Framework

Practicum Output Document

Preamble

1. This document outlines opportunities and challenges related to the harmonisation of the Protocol on Digital Trade (the Protocol) under the African Continental Free Trade Area (AfCFTA), adopted in February 2024 with the African Union Data Policy Framework (referred to hereafter as the AUDPF), adopted in July 2022. Its objective is to identify challenges, propose actionable solutions, and contribute to the effective implementation of two critical annexes to the Protocol, supporting Africa's vision for a unified, inclusive, and sustainable digital economy, namely (i) cross-border data transfers and (ii) criteria for determining legitimate public reasons for disclosure of source code. We believe this document will be of value to the Secretariat of the AfCTA, member states, and other regional organisations including Regional Economic Communities (RECs).
2. The reflections and recommendations included in this document are the results of a collaborative effort amongst individuals from various stakeholder groups, including governments, members of Parliament, businesses, civil society, intergovernmental organisations, the media, research institutions and the technical community who participated in the 11th edition of the African School of Internet Governance (AfriSIG) held at the United Nations Economic Commission for Africa in Addis Ababa, Ethiopia, from 14 to 19 November 2024.
3. Its authors recognise the transformative potential of the AfCFTA in accelerating intra-African trade and boosting Africa's trading position in the global market. They also recognise the importance of aligning the Protocol with the AUDPF to avoid challenges related to policy misalignments and contribute to the development of digital infrastructure in the region. We believe that overcoming

these challenges will enhance regional integration, accelerate economic growth, and promote equitable development across all member states, particularly for marginalised communities.

Section A: General remarks on the AfCFTA Digital Protocol and the AUDPF

The adoption in February 2024 of the AfCFTA Digital Protocol by the 37th African Union (AU) Heads of State Summit has resulted in Africa's first region-wide digital trade framework, which spans 54 countries and covers the world's largest free trade area.

The Protocol envisions digitally-driven industrialisation in Africa by enabling an environment for digital commerce and innovation. It establishes harmonised digital trade rules and principles that can lower trade transaction costs, enhance access to regional markets, and stimulate digital entrepreneurship. It represents significant potential for Africa to establish a unified, interoperable single digital market and is in alignment with the AU's Agenda 2063 and Digital Transformation Strategy 2020–2030.

The AUDPF, developed in 2022, offers significant benefits for Africa's data governance. It provides guidance for navigating complex regulatory issues, supports intra-African digital trade, entrepreneurship, and innovation, and establishes safeguards against risks and potential harms arising from the digital economy. In particular, it supports cross-border data transfer, fostering innovation and expansion into new markets; requires upskilling, creating opportunities for professionals in the digital economy; ensures fair competition by preventing monopolistic behaviour in the digital economy; promotes the establishment of innovation hubs to foster collaboration among tech entrepreneurs, researchers, and policymakers; advances research and development in emerging technologies and protects intellectual property while allowing source code disclosure for compelling public interest reasons.

The AUDPF outlines a roadmap for managing data across Africa, emphasising a trusted, secure, and inclusive ecosystem that balances the benefits of data innovation with the need for privacy, security, and ethical governance. It seeks to harmonise policies across member states, fostering collaboration and interoperability essential for achieving the goals of the Protocol and establishing a Digital Single Market in the region.

Effective data governance is crucial for the success of the Protocol and for ensuring equitable economic policies. Aligning national data policies with this framework can support regional cooperation and the goals of AfCFTA, integrating personal and non-personal data to inform economic strategies and promote inclusivity. The alignment of the annexures in the Protocol with the AUDPF would be a key step towards addressing Africa's regulatory diversity by enabling a cohesive approach to cross-border data transfers, while also addressing concerns related to intellectual property rights, data protection and cybersecurity.

Comprehensive data protection laws, independent data protection authorities, and civil society empowerment are crucial for ensuring the protection of digital rights as are the development of co-jurisdictional frameworks that allow for effective governance of the digital economy. The AUDPF recognises that harmonising existing data policies to build trust in the ecosystem is complex. It nonetheless provides room for states to preserve their sovereign interests while designing and revising policies that serve the continent’s interests. In this way, it serves as a key reference resource for member states as they design and review their data governance policies and legal instruments, contributing to a unified, secure, and forward-thinking data governance landscape.

Implementation of the AUDPF necessitates collaboration among AU member states, private sector stakeholders, the technical community, and civil society organisations, ensuring that their respective interests and concerns are adequately addressed. The AUDPF also emphasises the importance of data sovereignty and ownership. It encourages countries to establish national data systems that empower local institutions and uphold the continent's digital independence. Balancing cross-border data flows with data sovereignty also requires upholding privacy and security to prevent misuse and breaches.

Cross-border data transfers intended to facilitate the free flow of data among African nations to support digital trade must not prioritise corporate interests over data sovereignty and the protection of personal information. Unrestricted data flows could allow private corporations to exploit African data markets without adequate safeguards, potentially leading to data exploitation and loss of control over sensitive personal information.

While the Framework is a strategic asset enabling development, challenges remain, such as disparities in implementation among member states, differing levels of digital readiness, and the need to muster the needed political will. There are also significant disparities in digital infrastructure and participation in the digital economy across African nations. The AUDPF is an important guiding tool that harmonises existing data governance frameworks and provides intersections between data rights and privacy while not compromising easy access to data and information.

Implementation of the Protocol must prioritise initiatives that bridge this divide by improving internet access and digital literacy. An approach that takes into account structural imbalances in power and access to resources and that prioritises the inclusion of excluded groups can also help bridge the digital divide and promote equitable trade opportunities, particularly for initiatives and enterprises led by women and located in rural communities. In this context, small and medium enterprises (SMEs) must be strongly highlighted and consideration given to the challenges they face, to ensure they benefit from the digital free trade in Africa.

The Protocol is set to spark a wave of industrialisation and diversification by reducing trade barriers and addressing key enablers of digital trade such as cross-border data transfers, e-commerce regulations, and digital taxation. In this regard, there is also a need to fast-track the implementation of the Pan African Payment System (PAPPS). The AUDPF, the Protocol, and other data governance initiatives collectively serve as important components in Africa’s regional integration and pursuit of digital transformation, specifically in areas of policy-making, innovation, and driving economic growth.

Section B: Challenges and concerns

We recognise that harmonising the Protocol with the AUDPF faces critical challenges. Key among these is the disparity in policies and regulations across member states, particularly concerning data protection, privacy, cybersecurity, and digital taxation. Divergent national laws create inconsistencies that impede the development of a unified digital trade environment. Policies on cross-border data flow further complicate harmonisation, with many countries imposing restrictions driven by concerns over data sovereignty and security.

While the Protocol promotes removing barriers to data flows, its allowance for restrictions based on legitimate concerns introduces ambiguities that could hinder regional integration and preferential access to data for Africans, as envisioned by the AUDPF. This creates an extra layer of regulatory complexity, potentially burdening governments and delaying implementation.

Many countries have disparate laws regarding data protection, which complicates compliance for businesses operating across borders. This inconsistency can lead to legal uncertainties and increased operational costs for companies trying to navigate multiple regulatory environments.

The Protocol’s provision that African countries should not require source code disclosure aligns with fostering innovation and attracting foreign investment. However, we believe this position requires nuanced consideration to balance economic interests with strategic and security concerns. While blanket prohibitions on source code disclosure protect proprietary technologies, they may limit the ability of governments to ensure that digital products meet security and ethical standards. This is particularly critical in sectors like healthcare, finance, and national security, where vulnerabilities in software could have severe consequences.

The lack of clarity around the non-disclosure of source codes also poses significant challenges. The current stance of the protocol discouraging mandatory disclosure raises concerns about accountability and fairness, especially when negotiating with large foreign technology providers. Furthermore, disparities in digital infrastructure and connectivity across the continent exacerbate inequalities in adopting harmonised policies. Limited stakeholder engagement, particularly with the private sector, civil society, and marginalised groups, undermines inclusivity, while insufficient emphasis on gender equity and digital rights risks perpetuating inequalities. Over-reliance on foreign technology providers, such as cloud services, further challenges African digital sovereignty.

Cross-Border Data Transfers and disclosure of source codes should take place with consideration of the following:

a. Protecting data privacy and security and emphasising the need for safeguards to ensure personal data is handled responsibly across borders.

b. Preventing data exploitation by ensuring that the extraction of data from developing countries without adequate economic benefits or safeguards for sovereignty, is prevented.

c. The impact of potential inequalities in digital trade that favour multinational tech companies over local startups, small businesses, and marginalised groups to ensure inclusivity and equity.

d. Clear criteria for determining legitimate public reasons for disclosure of source code.

e. Ensuring governments have the right to demand disclosure of source code in cases where public safety, digital rights, or regulatory oversight are at stake.

f. Recognising the importance of protecting intellectual property but rejecting blanket protections that may shield harmful practices or reduce consumer trust in balancing innovation with oversight.

g. Educating citizens through awareness campaigns on their digital rights, while advocating for inclusive policies and fair data-sharing agreements can address inequalities and support Africa's digital transformation by strategically engaging with these frameworks.

Multi-stakeholder collaboration is crucial and can drive actionable recommendations on digital inclusion, innovation, and the ethical use of emerging technologies. Stakeholders must also champion digital inclusion by promoting equitable access to ICTs, affordable internet, and digital skills development, particularly for marginalised groups such as women, rural populations, and people with disabilities.

Many African countries lack the necessary resources and institutional capacity to implement comprehensive data protection laws effectively. This gap can lead to uneven enforcement of regulations, creating a competitive disadvantage for businesses in regions with weaker regulatory frameworks. For instance, a significant hurdle in harmonising data governance is the lack of clarity regarding data protection and ownership responsibilities. This ambiguity can hinder businesses from confidently investing in data-driven innovations, as they may be uncertain about their rights and responsibilities over the data they collect and process. Additionally, it creates hesitancy for businesses about data-driven innovation and moving or sharing data across borders as they may fear breaching rights or regulations in another jurisdiction.

Without strong digital security laws, regulations, and practices within each country, the harmonisation of data protection and digital protocols across the continent will expose businesses to growing cybercrime, not only within the continent but also from other regions. Without addressing these barriers, efforts to harmonise the AfCFTA Digital Trade Protocol with the AUDPF risk fragmentation, diminishing the potential of digital trade to drive transformative regional integration in Africa.

The AUDPF provides general guidance on cross-border data transfers but lacks specificity for operationalising these principles within the AfCFTA framework. Implementation is ambiguous, and without clear standards, the technical processes for ensuring data protection during cross-border transfers are left to no interpretation, increasing risks of non-compliance. Countries with stricter cross-border transfer rules may create barriers to trade, undermining the goals of the Protocol.

Balancing Innovation with regulation: In balancing privacy protections with fostering digital innovation and trade. "Personal data collected on the territory of a State Party may only be transferred to another State Party with the prior authorisation of the data protection authority" Overtly strict data protection rules may stifle innovation, particularly for start-ups and SMEs that lack the resources to comply, but weak or inconsistent regulations may also expose businesses and individuals to data privacy and security vulnerabilities.

Criteria for Source Code Disclosure should ensure transparency as this is essential to foster trust and innovation. However, it's important to balance public interests with the risks of hindering innovation and exposing businesses to unfair competition

The annex to the Protocol concerning the disclosure of source code focuses on protecting intellectual property while allowing for exceptions under specific public interest conditions to ensure that businesses are not forced to disclose proprietary software code as a prerequisite for market access. However, such broad protections may limit oversight, especially in areas like cybersecurity, algorithmic transparency, and digital rights.

The annex does not clearly define 'legitimate public interest reasons' that would permit governments to require source code disclosure, particularly in scenarios involving public health, safety, and welfare. While this lack of clarity currently diverges from practices seen in regions like Europe, which enforces stricter digital regulations for transparency, there is an opportunity for future alignment with best practices. This alignment would be essential for African states as we seek to effectively balance digital trade with the protection of data, including personal data for individuals participating in digital trade.

At the same time, rules on cross-border data flows and access to source code that aim to facilitate free data flow and digital trade within the continent, should not inadvertently reinforce the dominance of foreign (non-African) tech companies in Africa, potentially hindering technology transfer crucial for developing Africa's emerging digital economy.

States must provide safeguards through their domestic legislation and policies for African industries, particularly small and medium-sized enterprises. They should also adopt measures that aim to encourage technology transfer, such as mandating or incentivizing transfer agreements as part of market access conditions for businesses linked to non-African countries when justifiable, and strengthen competition laws to prevent monopolistic tendencies or practices by foreign businesses (including tech giants) that stifle African innovation.

Section C: Proposals and recommendations

The following proposals and recommendations are intended to assist the AfCTA Secretariat, member states, other implementing agencies, individual businesses, and all other stakeholders, in the effective implementation and further development of the Protocol in a manner that is harmonised with the AUDPF.

General recommendations

We recommend:

1. Investing in capacity-building initiatives. Establish regional mechanisms to provide technical assistance and specialised training for regulators and stakeholders, including business entities. This would support member states in implementing effective data governance policies and assist them in developing the necessary infrastructure for the Protocol's implementation. The establishment and strengthening of regional mechanisms for capacity building is crucial. These would provide technical assistance to member states in implementing the Protocol and developing the necessary infrastructure for data governance.
2. Strengthen the implementation mechanism of the Protocol: The implementation mechanism of the AfCFTA Digital Trade Protocol, as currently devolved to a committee of the AfCFTA Secretariat, appears to have some weaknesses. We propose establishing a dedicated implementation body within the Secretariat, with a specific mandate to oversee the execution of the Protocol. This body should have the authority to monitor compliance, provide technical support, and address disputes.
3. Develop comprehensive national data governance legislation: Countries are urged to establish national laws on personal data protection that align with the principles outlined in the AU Malabo Convention. This legislation should prioritise well-defined data governance structures that enhance trust in digital environments. Ensuring a balance between trade facilitation and data sovereignty: Develop policies that align international trade facilitation efforts with the need to protect national data sovereignty.
4. Ensure that national data protection laws explicitly include provisions to prevent data exploitation. These laws should include safeguards to ensure that data extracted from African countries yields significant economic benefits and sovereignty protection.
5. The promotion of interoperability and open data standards: We recommend developing mechanisms for interoperability and setting open data standards. This would facilitate non-personal data sharing, including sharing among researchers and entrepreneurs while ensuring compliance with privacy principles.

6. Launching awareness campaigns. Develop initiatives to educate citizens about their digital rights.
7. Invest in an enabling environment for digital trade to flourish. This include ensuring equitable access to ICTs, affordable internet, and digital skills training, particularly for marginalised groups.
8. Ensuring Inclusivity and Equity: Identify and highlight the impact of potential inequalities in digital trade that favour multinational tech companies over local startups, small businesses, and marginalized groups. To address these inequalities, local innovation should be encouraged, fair competition should be promoted, and regulatory support should be provided for local businesses to facilitate equitable access to digital trading opportunities.

Recommendations on cross-border data flows

9. We recognise the importance of removing barriers to cross-border data flows to facilitate digital trade and economic integration under the AfCFTA. However, the current provision in the protocol allowing countries to restrict such flows based on "legitimate concerns" introduces ambiguity and potential regulatory challenges. This condition places an additional regulatory burden on several stakeholders, including parliaments, as they are tasked with defining and overseeing what constitutes "legitimate concerns." The absence of clear criteria creates a risk of inconsistent interpretations across member states, potentially undermining the harmonisation goals of the protocol. Moreover, the lack of clarity may discourage investment and innovation by creating uncertainty for businesses operating across borders. To address this, we propose the following additions to the annex on cross-border data flows:

   9.1 Define "Legitimate Concerns": Provide a clear and narrow definition of legitimate concerns, including specific grounds such as national security, public health, and protection of fundamental rights.

   9.2 Establish mechanisms for oversight, compliance, and support for implementation. This could involve the establishment of an oversight body under the AfCFTA Secretariat to review, advise on, and if appropriate, approve any restrictions on cross-border data flows to ensure compliance with the protocol.

   9.3 Mandate Transparency: Require member states to publicly disclose the rationale and evidence for imposing restrictions, ensuring accountability.

   9.4 Encourage Proportionality: Specify that any restrictions must be the least restrictive means to address legitimate concerns, in line with international standards.

We also recommend:

10. The facilitation of mutual recognition agreements among member states to acknowledge and recognize each other’s data protection frameworks, thereby enabling trusted and seamless data flows

11. The integration of markets and standardisation of online payment and taxation systems, to ease cross-border data flows and trade while ensuring that no customs duties are imposed on digital products as per the Protocol.

Recommendations on source code disclosure

Access to source code should be allowed for national security, public safety, and regulatory compliance. Oversight by judicial or independent bodies is necessary to protect against arbitrary actions, and confidentiality agreements should be mandated to protect intellectual property. Clear and transparent processes for requesting source code must be established to prevent misuse.

We recommend:

12. The introduction of Conditional Disclosure: Allow governments to require source code disclosure for specific, narrowly defined purposes, such as cybersecurity audits or public safety, under strict confidentiality agreements.
13. Utilise the dispute resolution mechanisms within the Protocol to address conflicts arising from source code disclosure requests, ensuring fairness and consistency in decision-making.
14. Establish guidelines for when and how source code can be reviewed to ensure consistency across member states and prevent abuse.
15. Promote the use of open standards and open-source solutions for government procurement to enhance transparency, reduce dependency on proprietary technologies, and foster innovation.
16. Enhance transparency and accountability by encouraging governments to adopt frameworks that allow them to request the disclosure of source codes when necessary to protect public safety, digital rights, or ensure regulatory compliance.
17. Balance Innovation with Oversight: Safeguard intellectual property rights while opposing blanket protections that could enable harmful practices or erode consumer trust.

These balanced approaches to cross-border data flows and source code disclosure ensure the Protocol aligns with the goals of the AUDPF while safeguarding African interests and addressing legitimate concerns. As parliamentarians, governments, civil society, members of business, the technical community and the media as well as researchers and international organisations, we are committed to refining these provisions to contribute to a robust and enforceable cross-border data governance framework that supports Africa’s digital transformation.

Conclusions

This collaboration marks a defining moment in Africa's vision to establish a unified, inclusive and sustainable digital market that strengthens regional integration, advanced, economic growth, and supports equitable development across member states. While we recognize the immense potential of both the protocol and the AUDPF, we also understand the complexities of harmonising policies across diverse, legal and regulatory landscapes. Addressing challenges, such as disparities in national data protection frameworks, balancing data sovereignty with the free flow of information, and ensuring the protection of digital rights remains critical. We must continue to navigate these challenges carefully ensuring that digital trade is not only facilitated, but it does so in a way that respects the sovereignty of AU member states and safeguards the interests of all stakeholders.

The proposals and recommendations within this document offer actionable steps to overcome these challenges, focusing on creating a clear, cohesive framework for cross-border data transfers and source score disclosure.

As we move forward, we must maintain a collaborative multi-stakeholder approach that includes government businesses, civil society, and technical experts. Only through concerted efforts and continuous dialogue can we ensure that the AfCFTA and the AUDPF fulfil their transformative potential. We remain committed to working with all parties to refine and implement the necessary frameworks that will drive a digital transformation and show that the benefits of digital trade are distributed, equitably, and sustainably across the continent.