

GUARDING THE GRID: DATA PRIVACY, CONSUMER PROTECTION, AND AFRICA'S ROADMAP TO DIGITAL SECURITY

Author: Kelechukwu Uzoka, LL.M, MCI Arb. (UK), ABR, Notary Public

Affiliation: Lead Partner, K&C Partners Law Firm, Victoria Island, Lagos, Nigeria

Contact: kcuzoka@gmail.com, kuzoka@kcpartnerslaw.com, +234-8067310024

Website: www.kcpartnerslaw.com

LinkedIn: <https://www.linkedin.com/in/kelechukwuuzoka/>

Abstract

As Africa's digital economy expands, the continent's data protection and cybersecurity architecture is being tested by the same forces reshaping its security and economic landscape: cross-border data flows, rising cybercrime, and the growing use of personal data in both commercial and security contexts. This paper examines the entry into force of the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) in June 2023 and the African Union Continental Artificial Intelligence Strategy adopted in July 2024 as twin continental turning points, and asks whether these, alongside national instruments such as Nigeria's Data Protection Act 2023, South Africa's Protection of Personal Information Act, and comparable legislations, offer a coherent legal roadmap for digital security or merely a patchwork of overlapping obligations.

The paper argues that data privacy and consumer protection law must be understood not as a peripheral regulatory concern but as a frontline instrument of Africa's broader resilience agenda, safeguarding critical infrastructure, protecting citizens from exploitation in vulnerable digital markets, and underpinning the trust necessary for AfCFTA-driven digital trade to succeed. It considers the tension between security-justified data access and citizens' privacy rights, the enforcement gaps left by under-resourced national data protection authorities, and the risks posed by regulatory fragmentation across regional economic communities.

Drawing on the Malabo Convention, the AU AI Strategy, comparative national legislation, and AU digital policy instruments, the paper proposes a framework for harmonising data privacy and consumer protection standards across Africa, positioning digital security not as a constraint on growth but as a precondition for the continent's sustainable economic and security stability.

1. Introduction

Africa's digital economy is no longer a peripheral story of leapfrogging infrastructure. It is now central to how the continent trades, governs, and defends itself. Mobile money, e-government portals, digital lending platforms, e-commerce sites, and increasingly, artificial intelligence tools used by security agencies, all run on the same underlying resource: personal data. That convergence is what this analysis sets out to trace. It is not a coincidence that the same decade which saw Africa's digital economy accelerate also saw its data governance architecture reach two decisive milestones. The African Union Convention on Cyber Security and Personal Data Protection, commonly called the Malabo Convention, entered into force in June 2023, nine years after its adoption.¹

Just over a year later, in July 2024, the African Union Executive Council adopted the Continental Artificial Intelligence Strategy, a soft-law instrument that places safety, security, and economic transformation at the centre of Africa's approach to AI governance.²

These two instruments, taken together, are the twin continental turning points this paper is built around. The underlying question is a deliberately unsettled one: do the Malabo Convention, the AU AI Strategy, and the growing body of national legislation they sit alongside add up to a coherent legal roadmap for digital security, or do they simply multiply the number of overlapping obligations an African state, business, or citizen must somehow navigate at once? The central argument advanced here is that data privacy and consumer protection law are not a peripheral compliance concern sitting apart from Africa's security and economic resilience agenda. They are a frontline instrument of it. Personal data is now the raw material of both economic forecasting and security intelligence; a legal architecture that fails to protect it fails, by extension, to protect the resilience it is meant to enable.

What follows unfolds across seven further parts. Part 2 examines the Malabo Convention as the continental backbone of data protection law, including the criticisms that have followed it into force. Part 3 turns to the AU Continental AI Strategy and the point at which AI governance and data protection law become inseparable, particularly in the security domain. Part 4 undertakes a comparative survey of national implementation across six jurisdictions: Nigeria,

¹African Union, 'African Union Convention on Cyber Security and Personal Data Protection' (au.int)

<<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>> accessed 7 August 2026.

²African Union, 'Continental Artificial Intelligence Strategy' (au.int, 2024)

<<https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>> accessed 7 August 2026.

South Africa, Kenya, Rwanda, Ghana, and Egypt. Part 5 considers data privacy as a form of consumer protection, using Nigeria's regulation of digital lending as a worked example. Part 6 examines the relationship between fragmented data governance and the economic integration goals of the African Continental Free Trade Area. Part 7 sets out recommendations for harmonisation, before Part 8 concludes.

2. The Continental Framework I: The Malabo Convention

The Malabo Convention has an unusually long history for an instrument only recently brought to life. First drafted in 2011 and adopted by the AU Assembly at its Twenty-Third Ordinary Session in Malabo, Equatorial Guinea, on 27 June 2014,³ it could not enter into force under Article 36 until fifteen-member states had ratified it — a threshold that took nearly a decade to reach. Mauritania's ratification on 9 May 2023 finally triggered entry into force thirty days later, on 8 June 2023.⁴

The Convention is deliberately broad, built around three pillars: the regulation of electronic transactions, the protection of personal data, and cybersecurity and cybercrime.⁵ On data protection, it requires every state party to establish a national legal framework built on core principles of consent, lawfulness, confidentiality, and transparency, overseen by an independent authority with power to monitor compliance.⁶ On cybersecurity, it obliges each state to adopt a national policy and strategy, to criminalise a defined range of cyber offences, and to build the institutional capacity to detect and respond to threats while cooperating across borders on investigation and prosecution.⁷

That breadth is also the Convention's most persistent criticism. Commentators have argued that by bundling data protection, e-commerce, and cybercrime into a single instrument, the

³Andrew Gakiria and Tevin Mwenda Gitonga, 'What is the Malabo Convention?' (Diplo, 2025)

<<https://www.diplomacy.edu/blog/what-is-the-malabo-convention/>> accessed 7 August 2026.

⁴'Malabo Convention' (Wikipedia) <https://en.wikipedia.org/wiki/Malabo_Convention> accessed 13 August 2026.

⁵Shamaa Sheik, 'AU Convention on Cyber Security and Personal Data Protection | Malabo Convention' (Michalsons)

<<https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281>> accessed 7 August 2026.

⁶ALT Advisory, 'The Malabo Roadmap: Approaches to Promote Data Protection' (dataprotection.africa, September 2022)

<https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf> accessed 9 August 2026.

⁷'Economic Community of West African States' (CCDCOE) <<https://ccdcoc.org/organisations/ecowas/>> accessed 9 August 2026.

Convention effectively stacks human rights law, criminal law, and commercial law on top of one another, with no clear hierarchy and no dedicated mechanism to reconcile the tensions between them.⁸

Three further gaps matter for what follows. The Convention says little about cross-border data flows, an omission that becomes more consequential as African states pursue the kind of continental digital trade discussed in Part 6.⁹ It does not specify how national data protection authorities are expected to cooperate with one another, leaving a fragmented enforcement landscape even among states that have ratified the same treaty;¹⁰ and entry into force has, in any event, not translated into universal state practice. South Africa, for instance, remains a signatory that has not ratified the Convention at all, on the reasoning that its existing framework, the Protection of Personal Information Act, the Electronic Communications and Transactions Act, and the Cybercrimes Act, already gives substantive effect to most of Malabo's requirements.¹¹

That gap between ratification and functional compliance is instructive. The real measure of the Convention's success will not be the number of ratifications it eventually collects, but whether it succeeds in pulling divergent national frameworks toward a common baseline. Even the AU Commission has acknowledged as much, conceding that implementation guidelines, a model data protection law, and stronger institutional support for the Network of African Data Protection Authorities are needed if the Convention is to move from formal entry into force to practical effect.¹²

⁸Jimena Sofia Viveros Alvarez, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade' (EJIL:Talk!, 14 June 2023) <<https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>> accessed 9 August 2026.

⁹ALT Advisory, 'The Malabo Roadmap: Approaches to Promote Data Protection' (dataprotection.africa, September 2022) <https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf> accessed 9 August 2026.

¹⁰Jimena Sofia Viveros Alvarez, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade' (EJIL:Talk!, 14 June 2023) <<https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>> accessed 10 August 2026.

¹¹Shamaa Sheik, 'AU Convention on Cyber Security and Personal Data Protection | Malabo Convention' (Michalsons) <<https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281>> accessed 9 August 2026.

¹²ALT Advisory, 'Malabo Convention Set to Enter Force' (dataprotection.africa, 19 May 2023) <<https://dataprotection.africa/malabo-convention-set-to-enter-force/>> accessed 7 August 2026.

As of early 2025, only sixteen of the African Union's fifty-five member states, well under a third of the continent, had actually ratified the Convention,¹³ a figure Chatham House has singled out as a warning of how slow ratification can entrench exactly the fragmentation the Convention was meant to prevent. Nigeria, whose Data Protection Act 2023 is examined in detail in Part 4 and which has been among the most vocal African states pushing for a global cybercrime treaty at the United Nations, has itself not ratified Malabo, alongside Algeria, another state that led on the UN process. A continent that can mobilise coordinated diplomatic pressure for a global cybercrime instrument, while its own flagship regional economies decline to ratify the equivalent regional one, exposes a credibility gap that non-African treaty partners are unlikely to overlook.

On substance, the Convention does grant data subjects a reasonably comprehensive set of rights, including rights to information, access, objection, and erasure, set out across a run of articles from 9 to 23. The difficulty is not the absence of rights on paper. It is the absence of any continental mechanism to make those rights operable across borders.¹⁴ No cooperative enforcement framework links the national data protection authorities that ratifying states are required to establish, so a data subject whose rights are violated by a controller operating from a different ratifying state has no clear continental recourse beyond whatever bilateral cooperation the two national authorities happen to arrange informally.

There is also a political-economy dimension to the Convention's stalled momentum that is easy to miss if the analysis stays purely doctrinal. Commentary on the slow uptake has observed that the resulting policy inertia has left many African states operating, in practice, within data governance terms effectively set by foreign technology companies based in China, the United States, and the European Union, rather than by any African-authored standard.¹⁵ On this reading, the cost of continued non-ratification is not merely fragmented domestic enforcement;

¹³Chatham House, 'The AU Can Help African Countries Adopt the UN Cybercrime Convention. But the Challenges Are Significant' (Chatham House, 31 October 2025) <<https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant>> accessed 6 August 2026.

¹⁴'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade' (Academia.edu) <https://www.academia.edu/103386834/The_African_Union_s_Malabo_Convention_on_Cyber_Security_and_Personal_Data_Protection_enters_into_force_nearly_after_a_decade_What_does_it_mean_for_Data_Privacy_in_Africa_or_beyond> accessed 6 August 2026.

¹⁵ALT Advisory, 'The Malabo Roadmap: Approaches to Promote Data Protection' (dataprotection.africa, September 2022) <https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf> accessed 6 August 2026.

it is the continued absence of continental leverage over the terms on which African personal data is processed by the platforms that dominate the continent's digital markets.

For states currently weighing accession, such as Kenya, which retains a national data protection framework broadly comparable to the Convention's requirements but has not yet ratified, the practical pathway is not a leap into unfamiliar territory. It is closer to a domestication exercise: mapping the overlap between existing national law and the Convention's requirements, identifying specific gaps, and building the institutional capacity of bodies such as national data protection authorities and cybersecurity response teams to carry the additional cooperative obligations ratification would bring.¹⁶ The absence of urgency behind that exercise across most of the continent, nearly three years after entry into force, remains the Convention's central unresolved problem.

3. The Continental Framework II: The AU Continental Artificial Intelligence Strategy

If the Malabo Convention is the continent's data protection backbone, the Continental Artificial Intelligence Strategy is the newer instrument testing whether that backbone can bear new weight. Adopted by the AU Executive Council in July 2024 following a period of stakeholder consultation, the Strategy takes what it describes as a people-centric, development-oriented, and inclusive approach to AI governance, built around five focus areas: harnessing AI's benefits, building AI capabilities, minimising risks, stimulating investment, and fostering cooperation.¹⁷

These focus areas translate into fifteen action points addressing societal, ethical, security, and legal challenges associated with AI, including a call for member states to adopt technical standards for the safety and security of AI systems, and to develop regulatory frameworks specifically addressing the risks posed by advanced AI systems.¹⁸

¹⁶ 'Accession to the Malabo Convention and the Future of Data Governance in Kenya' (Vellum Kenya, 1 October 2025) <<https://vellum.co.ke/accession-to-the-malabo-convention-and-the-future-of-data-governance-in-kenya/>> accessed 7 August 2026.

¹⁷ Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (FPF, 18 November 2024) <<https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 8 August 2026.

¹⁸ Brenda Mwale, 'AI and Counter-Terrorism in Africa: Assessing the Role of the African Union's Continental AI Strategy' (GNET, 26 June 2025) <<https://gnet-research.org/2025/06/26/ai-and-counter-terrorism-in-africa-assessing-the-role-of-the-african-unions-continental-ai-strategy/>> accessed 8 August 2026.

The security dimension of the Strategy is not abstract. Africa's security agencies are already turning to AI to strengthen intelligence gathering, improve surveillance, and disrupt propaganda networks run by extremist and criminal groups.¹⁹

The same technology, however, is being adopted by the actors it is meant to counter. Reporting indicates that a group linked to al-Qaeda organised a workshop in 2024 specifically to build its members' skills in using AI and related software for operational purposes, a marked shift from the more experimental, low-sophistication use of AI by armed groups observed as recently as 2023.²⁰

This dual-use dynamic is precisely why AI governance cannot be treated as a policy area separate from data protection. Predictive threat analysis, surveillance systems, and intelligence-gathering tools of the kind envisaged in the AU Strategy all depend on processing large volumes of personal data, communications metadata, biometric information, location data, at a scale and speed the Malabo Convention's drafters could not have anticipated in 2014. Where the data protection standards governing that processing are weak, inconsistently enforced, or entirely absent at the national level, the security benefits AI promises come bundled with a proportionate expansion of surveillance risk and potential rights abuse. The Strategy itself does not operate in a vacuum on this point: existing data protection and cybersecurity legislation is expected to supply much of the regulatory scaffolding within which AI governance in Africa will actually operate.²¹

The economic dimension of the Strategy is framed with similar ambition. AI is positioned as a strategic asset for accelerating Agenda 2063 and the Sustainable Development Goals, with

¹⁹AU Strategy Guides AI Use as 'Technology Grows' (Africa Defense Forum, 5 August 2025) <<https://adf-magazine.com/2025/08/au-strategy-guides-ai-use-as-technology-grows/>> accessed 8 August 2026.

²⁰Brenda Mwale, 'AI and Counter-Terrorism in Africa: Assessing the Role of the African Union's Continental AI Strategy' (GNET, 26 June 2025) <<https://gnet-research.org/2025/06/26/ai-and-counter-terrorism-in-africa-assessing-the-role-of-the-african-unions-continental-ai-strategy/>> accessed 10 August 2026.

²¹Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (FPF, 18 November 2024) <<https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 10 August 2026.

government and financial-sector applications, including forecasting tools intended to strengthen resilience against economic shocks, identified as priority use cases.²²

Yet the institutional foundation for this ambition remains uneven. As of mid-2025, only thirteen African countries had adopted a national AI strategy or draft AI policy, meaning the AU Strategy is, for most of the continent, the only AI governance instrument currently in existence at any level.²³

A parallel study assessing Africa's readiness for AI safety governance found a similarly uneven picture beneath the surface: thirty-six of Africa's fifty-five countries have enacted a data protection law of some kind, and thirty-nine have dedicated cybersecurity or cybercrime legislation, foundational instruments that the study argues could and should be used as a starting point for AI safety governance, rather than starting the AI conversation from a blank page.²⁴

That is the broader argument this paper advances: AI governance in Africa is not a green field. It is, whether policymakers frame it this way or not, an extension of the data protection and cybersecurity architecture that already exists, however unevenly. Treating the Malabo Convention and the AU AI Strategy as two separate policy conversations, run by different institutional stakeholders on different timelines, risks duplicating effort in some areas while leaving the connective tissue between them, particularly around lawful processing standards for AI-driven security tools, dangerously undertheorised.

The Strategy's own drafters appear aware of this connective tissue, at least in principle. Analysis of the security dimension of the Strategy has noted that it explicitly calls on member states to strengthen their national cybersecurity systems in line with the Malabo Convention

²²Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (FPF, 18 November 2024) <<https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 8 August 2026.

²³'The Global Majority in International AI Governance' (arXiv, 2025) <<https://arxiv.org/pdf/2601.17191>> accessed 10 August 2026.

²⁴'Toward an African Agenda for AI Safety' (arXiv, 2025) <<https://arxiv.org/pdf/2508.13179>> accessed 10 August 2026.

and other continental frameworks, so the linkage argued for here is one the text itself gestures toward, even if it has not yet been operationalised in practice.²⁵

That same analysis is, however, sharply critical of how far the Strategy actually goes on security specifically. It observes that the Strategy operates as a voluntary guiding framework carrying no binding obligations, meaning implementation will vary according to each member state's political will rather than any enforceable continental standard, and that it stops short of setting out detailed counterterrorism measures or practical defensive guidelines for integrating AI into national and regional security operations, a gap the same commentary describes as particularly concerning given how many African states lack the technical expertise and funding needed to build serious AI-enabled security infrastructure in the first place.²⁶

The Strategy's implementation timeline compounds this concern. It sets a five-year horizon running from 2025 to 2030, structured in two phases: an initial phase from 2025 to 2026 focused on establishing governance frameworks, developing strategic documents, mobilising resources, and building an AI advisory board and centres of excellence, followed by a formal review in 2027, before a concluding phase from 2028 to 2030 that is meant to deliver the Strategy's core projects and actions. As with AU strategies generally, member states are not compelled to adopt implementing legislation on any particular timeline; the Strategy exerts influence over national policy design rather than binding force.²⁷

Early implementation data suggests the gap between ambition and delivery is already wide. An analysis of the Strategy's first eighteen months of implementation, covering July 2024 to October 2025, found stark geographic concentration in how AI-related funding and capacity-building activity has actually landed on the continent, with the large majority of measured funding activity concentrated in only four countries, alongside minimal private-sector capital

²⁵'AI Policy Corner: AI and Security in Africa: Assessing the African Union's Continental AI Strategy' (Montreal AI Ethics Institute, 26 May 2026) <<https://montrealethics.ai/ai-policy-corner-ai-and-security-in-africa-assessing-the-african-unions-continental-ai-strategy/>> accessed 10 August 2026.

²⁶'AI Policy Corner: AI and Security in Africa: Assessing the African Union's Continental AI Strategy' (Montreal AI Ethics Institute, 26 May 2026) <<https://montrealethics.ai/ai-policy-corner-ai-and-security-in-africa-assessing-the-african-unions-continental-ai-strategy/>> accessed 11 August 2026.

²⁷'The AU Continental AI Strategy: Concrete Safety Proposals or High-Tech Hype?' (Ilina Program) <<https://www.ilinaprogram.org/blog/au-continental-ai-strategy-2024>> accessed 11 August 2026.

mobilised relative to the scale of investment the continent's own digital transformation targets assume is needed.²⁸

At a high-level AU policy dialogue on AI regulation held in Addis Ababa in May 2025, the AU Commissioner for Infrastructure and Energy noted that in the first quarter of 2025 alone, the overwhelming majority of AI startup funding raised on the continent went to just four countries, Kenya, Nigeria, South Africa, and Egypt, four of the six jurisdictions surveyed in Part 4 of this paper, and warned that AI risks widening Africa's digital divide rather than narrowing it if that concentration is not deliberately addressed.²⁹

A separate, more polemical assessment of the AU's AI governance efforts goes further, describing the Strategy and the accompanying Kigali Declaration on AI as remaining largely aspirational on paper, undermined by the absence of enforcement mechanisms and weak coordination among member states with varying degrees of political stability, notwithstanding the accompanying announcement of a proposed continental AI financing mechanism intended to combine public, private, and philanthropic capital at very substantial scale. Whatever the eventual fate of that financing mechanism, the more immediate constraint the same assessment identifies is structural: no African country had, as of the most recent available industry data, surpassed even a modest threshold of AI adoption, and the continent faces a severe shortage of specialised AI talent relative to its own stated development needs.³⁰

The cumulative picture from Parts 2 and 3 together is therefore not one of two isolated instruments moving at different speeds by accident. It is a single, recognisable pattern repeating at the continental level: an ambitious framework instrument, adopted with genuine political fanfare, whose practical force depends entirely on national-level resourcing, institutional capacity, and political will that is unevenly distributed across fifty-five very different states. The Malabo Convention took nine years to reach a ratification threshold that still, three years

²⁸From Aspiration to Implementation: The African Union AI Continental Strategy and the Development-Governance Paradox' (ResearchGate, 21 October 2025)

<https://www.researchgate.net/publication/396230260_From_Aspiration_to_Implementation_The_African_Union_AI_Continental_Strategy_and_the_Development-Governance_Paradox> accessed 11 August 2026.

²⁹African Union, 'Africa Declares AI a Strategic Priority as High-Level Dialogue Calls for Investment, Inclusion, and Innovation' (au.int, 17 May 2025) <<https://au.int/en/pressreleases/20250517/africa-declares-ai-strategic-priority-investment-inclusion-and-innovation>> accessed 13 August 2026.

³⁰'Ambition or Inability: Assessing the African Union's Efforts to Establish AI Governance' (Future Center, 23 December 2025) <<https://futureuac.com/en-US/Mainpage/Item/10684/ambition-or-inability-assessing-the-african-unions-efforts-to-establish-ai-governance>> accessed 14 August 2026.

on, covers under a third of the continent. The AU AI Strategy, barely two years into its five-year implementation horizon, already shows the same geographic concentration problem that has long characterised Africa's broader digital economy. Neither gap is a reason to abandon either instrument. Both are reasons to treat the harmonisation and capacity-building recommendations set out in Part 7 as urgent rather than aspirational.

4. National Implementation: A Comparative Survey

The continental instruments examined in Parts 2 and 3 mean little unless they are tested against what national legislatures and regulators have actually built. This Part undertakes a deeper, six-country survey, spanning West, East, Southern, and North Africa, chosen deliberately for their variety: Nigeria and Ghana as ECOWAS states operating under the Supplementary Act discussed in Part 7; Kenya and Rwanda as East African states with two of the continent's most actively enforced regimes; South Africa as a Southern African state that has still not ratified the Malabo Convention; and Egypt as a North African state whose data protection law is only now, five years after enactment, acquiring the operational detail needed for enforcement. Read together, they show a continent whose national law is not uniformly behind the Malabo Convention and Policy, nor uniformly ahead of it, but moving at six visibly different speeds.

4.1 Nigeria

Nigeria's Data Protection Act took effect on 12 June 2023, days after the Malabo Convention itself entered into force, replacing the Nigeria Data Protection Regulation of 2019, which had been issued as subsidiary legislation by the National Information Technology Development Agency and lacked the statutory weight needed for robust enforcement.³¹ The Act establishes the Nigeria Data Protection Commission as an independent regulatory authority with power to issue regulations and guidance, register and license data controllers and processors of major importance, conduct audits, investigate complaints, and issue enforcement orders.³²

Its enforcement powers have already been tested in practice. The Commission derives its authority principally from section 6 of the Act, which empowers it to monitor, investigate, and impose penalties, and section 48(4), which authorises administrative fines without the need for

³¹'Understanding the Nigeria Data Protection Act, 2023 (NDPA)' (Cookie Script) <<https://cookie-script.com/privacy-laws/nigeria-data-protection-act-2023>> accessed 15 August 2026.

³²'An Overview of Nigeria's Data Protection Act, 2023' (Securiti.ai) <<https://securiti.ai/overview-of-nigeria-data-protection-act/>> accessed 15 August 2026.

a prior court order.³³ Penalties are tiered by the size and significance of the data controller or processor, with fines for organisations of major importance capable of reaching two percent of the preceding year's annual gross revenue, or a fixed statutory minimum, whichever is higher³⁴ — and the Commission has not hesitated to use those powers against major commercial actors, imposing fines running into hundreds of millions of naira and tens of millions of dollars against prominent multinational operators found in breach of the Act.³⁵

What distinguishes Nigeria's regime is how quickly it moved from statute to active enforcement against globally significant defendants within roughly two years of assent, a pace matched on this survey only by Kenya's Worldcoin intervention discussed below. That pace has been possible in part because the NDPC did not have to build institutional legitimacy from nothing: it inherited registration infrastructure and a compliance culture already partially established under the 2019 NDPR, giving it a running start that some of the other jurisdictions surveyed here have lacked.

4.2 South Africa

South Africa's Protection of Personal Information Act received presidential assent in November 2013 but was only brought into full effect from 1 July 2020, with a one-year grace period before enforcement began in earnest on 1 July 2021.³⁶ It is enforced by the Information Regulator, an independent body with power to investigate complaints, conduct assessments, and issue enforcement notices; violations can attract fines of up to ten million rand or up to ten years' imprisonment, depending on severity.³⁷

³³'Data Protection Enforcement: Understanding the Powers of Regulatory Authorities' (Lex Luminar, 24 June 2025) <<https://lexluminar.com/data-protection-enforcement-understanding-the-powers-of-regulatory-authorities/>> accessed 17 August 2026.

³⁴'Nigeria Data Protection Act 2023: Key Features and Legal Framework' (PlanetWeb Solutions) <<https://planetweb.ng/key-features-of-the-nigeria-data-protection-act-2023/>> accessed 17 August 2026.

³⁵'Nigeria Data Protection Law: Complete NDPA Compliance Guide 2025' (Secure Privacy Blog) <<https://secureprivacy.ai/blog/nigeria-data-protection-law>> accessed 17 August 2026.

³⁶'South Africa's Protection of Personal Information Act (POPIA) Explained' (Termly) <<https://termly.io/resources/articles/south-africas-protection-of-personal-information-act/>> accessed 19 August 2026.

³⁷'The Protection of Personal Information Act (POPIA): A Comprehensive Guide' (Captain Compliance) <<https://captaincompliance.com/education/the-protection-of-personal-information-act-popia-a-comprehensive-guide-to-south-africas-data-privacy-regulation/>> accessed 17 August 2026.

The Regulator's enforcement record shows a body still building institutional muscle rather than one operating at full capacity: in 2024 it issued three POPIA enforcement notices while separately conducting more than thirty assessments under South Africa's access-to-information legislation, and it has publicly indicated it intends to approach Parliament for amendments that would strengthen its powers further.³⁸ Enforcement action taken so far has ranged from a notice against the South African Police Service over the improper sharing of gang-rape survivors' personal details on WhatsApp, to fines against private training institutions for unsolicited direct marketing.³⁹

The seven-year gap between assent and full effect, and the further gap before the Regulator's enforcement posture visibly hardened, illustrates a pattern distinct from Nigeria's: South Africa built a comprehensive, GDPR-comparable statute early, but the institution meant to enforce it took the better part of a decade to move from a body 'subject only to the law and the Constitution' on paper to one issuing enforcement notices against organs of state in practice. That gap between legislative completeness and institutional readiness is a better predictor of a jurisdiction's real data protection maturity than the age of its statute. South Africa's continued non-ratification of the Malabo Convention, discussed in Part 2, does not appear to reflect resistance to data protection as a principle; POPIA and its accompanying cybercrime legislation meet or, on some readings, exceed the Convention's substantive requirements. What it illustrates instead is a structural weakness in the continental architecture: a state can be fully compliant with the spirit of Malabo while remaining formally outside it, which does little to build the cross-border regulatory cooperation the Convention was designed to enable.

4.3 Kenya

Kenya's Data Protection Act, enacted to give effect to the right to privacy under Article 31 of the 2010 Constitution, entered into force on 25 November 2019 and established the Office of the Data Protection Commissioner as the country's independent enforcement authority.⁴⁰

³⁸Baker McKenzie, 'Regulators, Enforcement Priorities and Penalties: South Africa' (Global Data and Cyber Handbook) <<https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/south-africa/topics/regulators-enforcement-priorities-and-penalties>> accessed 18 August 2026.

³⁹'Safeguarding Privacy: South Africa's Protection of Personal Information Act (PoPIA)' (Infotrust, 5 September 2024) <<https://infotrust.com/articles/south-africas-protection-of-personal-information-act-popia/>> accessed 18 August 2026.

⁴⁰'Kenya: Data Protection Act Establishing Office of the Data Protection Commissioner Entered into Force' (Digital Policy Alert) <<https://digitalpolicyalert.org/event/27496-data-protection-act-2019-establishing-the-office-of-the-data-protection-commissioner-entered-into-force>> accessed 17 August 2026.

The Commissioner has the power to register data controllers and processors, investigate complaints, conduct audits, and impose administrative penalties, with fines capable of reaching five million Kenyan shillings or one per cent of an organisation's annual turnover.⁴¹

Complaints must be investigated and concluded within ninety days of being lodged, a statutory turnaround requirement that is unusually specific by regional standards and reflects a deliberate design choice to keep enforcement responsive rather than indefinitely pending.⁴²

Kenya's most consequential test of this framework came not from a routine compliance audit but from the ODPC's confrontation with Worldcoin, the biometric identity and cryptocurrency project that scanned the irises of hundreds of thousands of Kenyans through 'Orb' devices in exchange for digital tokens. A multi-agency investigation found that the consent obtained from data subjects did not comply with section 32 of the Act, that no Data Protection Impact Assessment had been conducted or submitted despite the processing of sensitive biometric data, and that the project's operating entity had continued collecting personal data without valid registration as a data controller.⁴³

The ODPC cancelled Worldcoin's registration certificate in September 2023 and issued an enforcement notice, but the Kenyan High Court subsequently found in a judgment reviewing the Commissioner's own conduct that the ODPC itself had been negligent in granting the original registration certificate without adequate diligence, and that by the time enforcement action was taken, the collected data had already moved beyond Kenyan jurisdiction to servers in the United States, Italy, and South Africa.⁴⁴

The matter escalated further in May 2025, when the High Court ruled Worldcoin's data gathering unlawful on constitutional grounds, citing breaches of the right to dignity and privacy under Articles 28 and 31 of the Kenyan Constitution, and ordered the deletion of all collected

⁴¹'Kenya Data Protection Act 2019 (DPA) Compliance Guide' (Securiti) <<https://securiti.ai/kenya-data-protection-act-dpa/>> accessed 19 August 2026.

⁴²'Office of Data Protection Commissioner Kenya: Compliance Guide' (Huduma Global Blog) <<https://hudumaglobal.com/blog/odpc-data-protection-act-kenya-compliance-guide>> accessed 17 August 2026.

⁴³'Office of Data Protection Commissioner Finds WorldCoin Violated Data Protection Regulations' (JURIST, 26 October 2023) <<https://www.jurist.org/news/2023/10/office-of-data-protection-commissioner-finds-worldcoin-violated-data-protection-regulations/>> accessed 17 August 2026.

⁴⁴Office of the Data Protection Commissioner v Tools for Humanity Corporation & 2 others (Worldcoin) Miscellaneous Criminal Application E315 of 2023; [2024] KEHC 312 (KLR) (Crim) (25 January 2024, Ruling) <<https://new.kenyalaw.org/akn/ke/judgment/kehc/2024/312/eng@2024-01-25>> accessed 18 August 2026.

biometric data under ODPC supervision, an order the regulator ultimately enforced by travelling to Germany in November 2025 to supervise the physical destruction of the data at its foreign storage location.⁴⁵

Commentators have described the case as a watershed moment for African data protection enforcement, not only for the scale of the fine exposure involved, but because it was the first instance of an African regulator securing the extraterritorial deletion of biometric data collected within its jurisdiction but exported abroad.⁴⁶

The ODPC's enforcement record beyond Worldcoin reinforces the picture of an active regulator, not a dormant one: a Nairobi school was fined approximately KES 4.55 million for publishing images of minors without parental consent, a comparatively modest case but one that signals the Commissioner's willingness to act against domestic institutions, not only high-profile international ventures.⁴⁷

4.4 Rwanda

Rwanda's Law No 058/2021 Relating to the Protection of Personal Data and Privacy was gazetted on 15 October 2021, giving institutions a twenty-four-month compliance runway before full enforcement began on 15 October 2023.⁴⁸ Rwanda took an institutional path distinct from every other jurisdiction in this survey: rather than establishing a freestanding data protection authority, it designated its existing National Cyber Security Authority as the law's supervisory body, formally launching a dedicated data protection office within that authority in March 2022.⁴⁹

This choice reflects a deliberate policy position, articulated by the NCSA's own Chief Cyber Security Standards Officer, that data protection and cybersecurity should be governed as a

⁴⁵'Worldcoin: Intrigues of Data Privacy' (Daily Nation, 1 December 2025) <<https://nation.africa/kenya/news/worldcoin-intrigues-of-data-privacy--5282596>> accessed 19 August 2026.

⁴⁶'Worldcoin Case a \'Watershed Moment\' for Data Protection in Kenya' (IAPP, 28 May 2026) <<https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya>> accessed 17 August 2026.

⁴⁷'When Yes Means No – A Look at Kenya's Evolving Data Protection Framework' (Afriwise Insights) <<https://insights.afriwise.com/blog/when-yes-means-no-a-look-at-kenyas-evolving-data-protection-framework>> accessed 18 August 2026.

⁴⁸'Rwanda' (Data Protection Africa Fact Sheet) <<https://dataprotection.africa/rwanda/>> accessed 22 August 2026.

⁴⁹'Who We Are' (Data Protection & Privacy Office, Rwanda) <<https://dpo.gov.rw/about-us/who-we-are>> accessed 23 August 2026.

single, unified discipline instead of as separate regulatory silos — the kind of institutional integration this paper has argued is missing at the continental level between the Malabo Convention and the AU AI Strategy.⁵⁰ The law is also considerably more protective on data localisation than any other jurisdiction surveyed here, requiring data controllers and processors to store personal data within Rwanda by default and permitting offshore storage only where the controller or processor holds a specific registration certificate issued by the NCSA.⁵¹

Rwanda had already ratified the Malabo Convention by 2019, when only twelve African states had done so several years before entry into force, and well ahead of its own domestic legislation, suggesting a level of early continental commitment not matched by others.⁵²

4.5 Ghana

Ghana's Data Protection Act 2012 is, by a decade, the oldest data protection statute examined in this survey, assented to on 10 May 2012 and in force since 16 October 2012, well over a decade before the Malabo Convention it now sits alongside actually entered into force.⁵³ The Act establishes the Data Protection Commission as an independent statutory body, requires mandatory registration of all data controllers before processing begins, and sets out eight binding data protection principles covering accountability, lawfulness, purpose specification, and data security.⁵⁴

Enforcement architecture is unusually granular for a law of its age: The Commission can issue enforcement notices carrying fines and, for the most serious offences such as the unlawful sale of personal data or repeated non-compliance, criminal sanctions of up to ten years' imprisonment.⁵⁵ Even so, age has not guaranteed uniform market compliance. Academic

⁵⁰'Rwanda Enacts Data Protection Law to Promote Rights to Privacy' (Paradigm Initiative, 5 December 2021) <<https://paradigmhq.org/rwandadataprivacy/>> accessed 23 August 2026.

⁵¹Law No 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (Rwanda) <<https://rwandalii.org/akn/rw/act/law/2021/58/eng@2021-10-15>> accessed 22 August 2026.

⁵²'Rwanda Enacts Data Protection Law to Promote Rights to Privacy' (Paradigm Initiative, 5 December 2021) <<https://paradigmhq.org/rwandadataprivacy/>> accessed 22 August 2026.

⁵³'Data Protection Act, 2012' (Wikipedia) <https://en.wikipedia.org/wiki/Data_Protection_Act,_2012> accessed 17 August 2026.

⁵⁴'Data Protection Compliance in Ghana' (TEMPLARS Law, 10 May 2023) <https://www.templars-law.com/app/uploads/2023/05/Data-Protection-Compliance-in-Ghana_final.pdf> accessed 17 August 2026.

⁵⁵'Data Protection Act, 2012 (Act 843) - Ghana' (Regulations.AI) <<https://regulations.ai/regulations/RAI-GH-NA-ACT8430-2012>> accessed 17 August 2026.

commentary has noted that major Ghanaian telecommunications providers have, at points, continued using subscriber mobile data in ways that sit uneasily with the Act's consent requirements under section 20(1), a reminder that a decade-old, well-designed statute is not, on its own, sufficient without sustained, well-resourced enforcement against the largest data controllers in the market, the same enforcement-capacity problem identified earlier in South Africa and, to a lesser extent, Nigeria.

Ghana's position within the continental architecture is also structurally interesting: it is simultaneously a member of the ECOWAS Supplementary Act framework discussed in Part 7 and a ratifying state of the Malabo Convention, giving it, on paper, the most layered set of overlapping regional and continental obligations of any jurisdiction in this survey.⁵⁶

4.6 Egypt

Egypt's Personal Data Protection Law No. 151 of 2020 was enacted on 13 July 2020 and took effect on 14 October 2020, establishing the Personal Data Protection Center under the Ministry of Communications and Information Technology as the country's supervisory authority, with power to license data controllers and processors, investigate breaches, and impose administrative sanctions.⁵⁷

Egypt's experience is the clearest illustration in this survey of the gap between a statute's enactment and its operational readiness. More than five years passed between the Law's entry into force and the issuance, by Ministerial Decree No. 816 of 2025, of the Executive Regulations needed to give the Center the operational detail required to actually license controllers, process applications, and enforce the Law at scale.⁵⁸

Under the Executive Regulations, organisations now have a further one-year grace period, with full enforcement expected only from 31 October 2026, meaning that more than six years will

⁵⁶Ghana's Data Protection Act 2012 (Act 843)' (ITLawCo, 28 January 2025) <<https://itlawco.com/focus-areas/data-protection-and-privacy/ghanas-data-protection-act-2012-act-843/>> accessed 18 August 2026.

⁵⁷Andersen Egypt, 'Translation of Law No. 151 of 2020' <<https://eg.andersen.com/translation-law-151-2020/>> accessed 20 August 2026.

⁵⁸Baker McKenzie, 'Egypt: Important Data Protection Update' (Baker McKenzie Insight, January 2026) <<https://www.bakermckenzie.com/en/insight/publications/2026/01/egypt-important-data-protection-update>> accessed 25 August 2026.

ultimately separate the Law's original enactment from the point at which it becomes fully enforceable against the ordinary run of Egyptian businesses.⁵⁹

Penalties, once the Law does bite, are substantial: administrative fines of up to EGP 5 million alongside potential imprisonment of more than six months for non-compliance, with a specific, narrower fine band of EGP 50,000 to EGP 500,000 reserved for violations attributable to the negligence of an organisation's designated Data Protection Officer.⁶⁰

Egypt's Law also rests on a constitutional foundation distinct from any other jurisdiction surveyed here: Article 57 of Egypt's 2014 Constitution independently guarantees the inviolability of private life and communications, meaning the 2020 Law operationalises a right that predates it by six years, a sequencing that stands in contrast to Kenya, where the constitutional right to privacy under Article 31 and the 2019 statute implementing it followed a similar but more compressed timeline.⁶¹

The five-year implementation lag is, on the argument made here, the most telling data point Egypt contributes to this survey. A state can enact data protection legislation broadly comparable in ambition to the GDPR, and still leave citizens and regulated businesses in a state of prolonged uncertainty if the executive machinery needed to operationalise it, licensing procedures, fee schedules, sector-specific guidance, is not built in step with the statute itself. The same risk attends the Malabo Convention at continental level, where entry into force in 2023 has not, on the evidence reviewed in Part 2, been matched by comparably fast-moving implementation guidance from the AU Commission.

Egypt's position cuts deeper than that, because it was not a Malabo laggard like South Africa or Nigeria. Egypt was among the fifteen founding ratifying states whose instruments of ratification brought the Convention into force in June 2023, ratifying the continental treaty years ahead of most of the continent discussed in Part 2. That a state which moved early and decisively on continental ratification could still leave its own domestic statute without functioning executive machinery for more than five years sharpens the claim running through

⁵⁹'Egypt Data Privacy Laws: PDPL Law 151/2020 and the 2025 Executive Regulations' (Recording Law)

<<https://www.recordinglaw.com/world-laws/world-data-privacy-laws/egypt-data-privacy-laws/>> accessed 25 August 2026.

⁶⁰'Egypt Data Protection Law' (PwC Middle East) <<https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/navigating-data-privacy-regulations/egypt-data-protection-law.html>> accessed 24 August 2026.

⁶¹'Egypt Data Privacy Laws: PDPL Law 151/2020 and the 2025 Executive Regulations' (Recording Law)

<<https://www.recordinglaw.com/world-laws/world-data-privacy-laws/egypt-data-privacy-laws/>> accessed 27 August 2026.

this analysis more than a simple non-ratifier would: ratification, whether of a continental convention or the passage of a domestic statute, is consistently the easy half of the problem. Building the institutional capacity to enforce what has been ratified or enacted is the harder half, and it is the half that Africa's data governance architecture, continental and national alike, has struggled with most.⁶²

4.7 A harmonisation problem, not a harmonisation solution

Read together, these six jurisdictions do not tell a single story; they tell at least four. Nigeria and Kenya show what fast, assertive enforcement against major domestic and international actors looks like within two to four years of a statute taking effect. South Africa and Egypt show the opposite: legally sophisticated statutes whose enforcement machinery took the better part of a decade, and in Egypt's case more than six years, to become fully operational. Rwanda shows a distinct institutional model, folding data protection into an existing cybersecurity authority rather than building a standalone regulator, alongside the strictest data localisation regime in this survey. Ghana shows that statutory age alone guarantees nothing: a law a decade older than the Malabo Convention itself still struggles with compliance among the country's largest data controllers.

A business, or an AI-driven security or forecasting tool of the kind discussed in Part 3, operating across Lagos, Nairobi, Kigali, Accra, Johannesburg, and Cairo simultaneously, does not face one African data protection regime. It faces six, each with its own registration thresholds, penalty structures, localisation requirements, and enforcement tempo, an outcome the Malabo Convention was explicitly designed to prevent but has not, on this evidence, yet achieved.

5. Consumer Protection in the Digital Space

Data privacy law rarely announces itself to ordinary citizens by that name. Most Africans encounter its absence, not its presence, through exploitative conduct in digital markets: unauthorised access to phone contacts, harassment of a borrower's family and colleagues, or the sale of personal information to third-party marketers. Nigeria's experience with digital lending platforms illustrates this connection clearly. Following a wave of complaints about the

⁶²The Malabo Convention: Africa's Cybersecurity and Data Protection Framework Explained' (African Researchers Magazine, 24 February 2025) <<https://www.africanresearchers.org/the-malabo-convention-africas-cybersecurity-and-data-protection-framework-explained/>> accessed 27 August 2026.

conduct of so-called loan apps, including social shaming of defaulting borrowers, unauthorised access to contact lists, and aggressive debt-recovery tactics that breached borrowers' data privacy rights, the Federal Competition and Consumer Protection Commission (FCCPC) issued its Limited Interim Regulatory and Registration Framework and Guidelines for Digital Lending in August 2022.⁶³

The Commission's intervention did not stop at soft guidance. It directed Google to remove non-compliant lending applications from the Play Store and instructed payment service providers to cease processing transactions for unregistered or investigated lenders, using its powers under sections 17, 18, and 163 of the Federal Competition and Consumer Protection Act 2018.⁶⁴

That interim framework has since matured into the Digital, Electronic, Online and Non-Traditional Consumer Lending Regulations 2025, which explicitly cross-references the Nigeria Data Protection Act's provisions on lawful processing and the prohibition of unauthorised disclosure, and imposes dedicated obligations on lenders regarding data protection, cybersecurity, and borrower information disclosure.⁶⁵

This is a clean illustration of the paper's central claim in miniature. Nigeria's consumer protection regulator did not treat data privacy as someone else's problem. It treated unauthorised data access and disclosure as the mechanism of consumer harm, and built its enforcement response, right down to platform-level takedowns, around that understanding. The Commission continues to maintain and publish a list of approved digital lenders and actively encourages consumers to transact only with registered platforms, an ongoing enforcement posture rather than a one-off intervention.⁶⁶

⁶³The FCCPC's Limited Interim Regulatory/Registration Framework and Guidelines for Digital Lending, 2022' (Mondaq, 7 October 2022) <<https://www.mondaq.com/nigeria/dodd-frank-consumer-protection-act/1237972/the-fccpcs-limited-interim-regulatory-registration-framework-and-guidelines-for-digital-lending-2022>> accessed 27 August 2026.

⁶⁴Analysis of FCCPC's Limited Interim Regulatory and Registration Framework and Guidelines for Digital Lending in Nigeria' (Lexology, 29 November 2022) <<https://www.lexology.com/library/detail.aspx?g=84f91798-86d1-4b3b-b092-f4d88dec68fc>> accessed 27 August 2026.

⁶⁵Nigeria's 2025 Consumer Lending Regulations: Key Frameworks and Guidelines' (SHQ Legal, 3 October 2025) <<https://www.shqlegal.com/publications/understanding-the-2025-digital-electronic-online-and-non-traditional-consumer-lending-regulations-in-nigeria>> accessed 27 August 2026.

⁶⁶Federal Competition and Consumer Protection Commission, 'Registration of Digital Money Lenders' (fccpc.gov.ng) <<https://fccpc.gov.ng/registration-of-digital-money-lenders/>> accessed 27 August 2026.

The broader lesson for African data protection authorities, most of which remain under-resourced relative to their statutory mandates, is that consumer protection regulators can be effective allies in enforcing data privacy norms even where a dedicated data protection authority lacks the capacity to act alone. Telecommunications regulation sits adjacent to this same terrain: network-level data practices, subscriber identity verification, and consent mechanisms for marketing communications all implicate the same underlying privacy interests, even where the enforcing regulator is a telecoms authority rather than a data protection commission. A coordinated approach between sectoral consumer regulators and data protection authorities, rather than siloed enforcement, is likely to do more for ordinary citizens than strengthening either regulator in isolation.

6. Cross-Border Data Flows and Economic Stability

The African Continental Free Trade Area's ambitions for digital trade cannot be separated from the data governance questions examined above. The AfCFTA Digital Trade Protocol, adopted by the AU Assembly in February 2024, is a landmark instrument covering electronic transactions, data protection and privacy, consumer rights, cybersecurity, digital inclusion, and cooperation on emerging technologies, with the explicit goal of reducing regulatory fragmentation across African states.⁶⁷

The Protocol's data governance provisions sit in tension with, rather than in simple alignment with, the Malabo Convention. Article 20 of the Protocol addresses cross-border data flows, while a separate Data Annex under Article 20(3) and provisions on personal data protection and cybersecurity in Articles 21 and 25 are carved out from the Protocol's general market-access disciplines.⁶⁸

Critics argue that the Protocol's cross-border data flow rules, including a most-favoured-nation style obligation requiring states to extend the same data flow concessions negotiated with non-African trade partners to fellow AfCFTA members, risk favouring established international technology platforms over the AU's own Data Policy Framework, which promotes a more

⁶⁷tralac Trade Law Centre, 'The OECD's New Index of Digital Trade Integration Shows Strong Gains from the AfCFTA's Digital Trade Protocol' (tralac, 2026) <<https://www.tralac.org/blog/article/16912-the-oecd-s-new-index-of-digital-trade-integration-shows-strong-gains-from-the-afcfta-s-digital-trade-protocol.html>> accessed 27 August 2026.

⁶⁸Research ICT Africa, 'Alignment Problems: The AfCFTA Digital Trade Protocol and AI' (Just AI, 2025) <https://researchictafrica.net/wp-content/uploads/2025/02/Alignment-problems-AfCFTA-digital-trade-protocol-AI_Just_AI_2025.pdf> accessed 28 August 2026.

equitable, protective approach to data governance for the benefit of least-developed African economies.⁶⁹

A more pointed critique goes further, arguing that the data transfer and source-code secrecy provisions negotiated into the Protocol echo digital trade rules that the United States itself has recently stepped back from at the multilateral level, a retreat driven by concerns about unchecked platform power over personal and sensitive data, and that African states are now being asked to accept terms that better-resourced economies no longer consider fit for purpose.⁷⁰

Whichever view is correct, the practical consequence is the same: African states are now negotiating data governance commitments on two separate tracks, a continental security and human-rights track running through the Malabo Convention, and a continental trade-liberalisation track running through the AfCFTA Digital Trade Protocol, without a clearly established mechanism for reconciling the two where they diverge.

7. Toward a Harmonised Framework: Recommendations

The evidence assembled in Parts 2 through 6 points toward five concrete recommendations, each aimed at closing a specific gap identified above, instead of restating harmonisation as a vague aspiration.

7.1 A model African data protection law, not another convention

The African Union Commission should prioritise development of a detailed model data protection law, built on the Malabo Convention's principles but drafted with the specificity needed for direct domestication by the roughly two-thirds of member states that, on the evidence in Part 2, have still not ratified the Convention nearly three years after entry into force. The absence of such a model is not a hypothetical gap; it has already been identified by practitioners working on continental implementation as a necessary next step, and the case for it is strengthened by the finding, above, that even flagship economies such as Nigeria and Algeria, states with the diplomatic capacity to lead a global cybercrime treaty process at the

⁶⁹Research ICT Africa, 'Alignment Problems: The AfCFTA Digital Trade Protocol and AI' (Just AI, 2025)

<https://researchictafrica.net/wp-content/uploads/2025/02/Alignment-problems-AfCFTA-digital-trade-protocol-AI_Just_AI_2025.pdf> accessed 27 August 2026.

⁷⁰'The AfCFTA's Digital Trade Rules Are Not Fit for Africa' (Afronomicslaw)

<<https://www.afronomicslaw.org/category/analysis/afctas-digital-trade-rules-are-not-fit-africa>> accessed 27 August 2026.

United Nations, have not ratified the regional instrument. A model law lowers the drafting burden that appears, on the evidence reviewed in Part 2, to be a genuine contributor to non-ratification, instead of leaving every legislature to negotiate the Convention's principles into domestic statute from first principles.⁷¹

7.2 An explicit institutional bridge between Malabo and the AI Strategy

The institutional link between the Malabo Convention's data protection architecture and the AU AI Strategy's security and economic ambitions needs to be made explicit rather than assumed. The Strategy already gestures toward this link, calling on member states to strengthen national cybersecurity systems in line with the Malabo Convention, but Part 3 found no operational mechanism translating that reference into practice. A joint AU Commission working group spanning both instruments, or a formal requirement that national AI strategies developed under the Strategy's guidance demonstrate compliance with Malabo-equivalent data protection standards before qualifying for AU-coordinated funding or technical support, would convert a textual cross-reference into an enforceable link. Given that Part 3 found AI-related funding and capacity-building activity concentrated overwhelmingly in four countries, Kenya, Nigeria, South Africa, and Egypt, four of the six states examined in the comparative survey above, this bridge should be piloted in those four jurisdictions first, where both the data protection infrastructure and the AI investment already exist to make the link testable within the Strategy's own 2025 to 2026 first implementation phase.⁷²

7.3 Strengthening the Network of African Data Protection Authorities as the enforcement bridge

The Network of African Data Protection Authorities, established in 2016 and now comprising national authorities from roughly twenty member states, is the one continental body already doing the cross-border cooperation work the Malabo Convention itself does not provide for. It has signed a memorandum of understanding with the Smart Africa Alliance specifically to support enforcement capacity and legislative drafting, and its own member commissioners

⁷¹ALT Advisory, 'Malabo Convention Set to Enter Force' (dataprotection.africa, 19 May 2023)

<<https://dataprotection.africa/malabo-convention-set-to-enter-force/>> accessed 28 August 2026.

⁷²From Aspiration to Implementation: The African Union AI Continental Strategy and the Development-Governance Paradox' (ResearchGate, 21 October 2025)

<https://www.researchgate.net/publication/396230260_From_Aspiration_to_Implementation_The_African_Union_AI_Continental_Strategy_and_the_Development-Governance_Paradox> accessed 17 August 2026.

have publicly called for deeper cooperation on enforcement, cybersecurity, and consumer protection across the continent.⁷³

The case for channelling AU resources through this Network rather than building new institutional architecture from scratch is strengthened by the findings in Part 4. Kenya's Data Protection Commissioner, whose office secured the extraterritorial destruction of Worldcoin's biometric data examined in Part 4, has herself used the Network's most recent conference to press for greater regulatory cooperation and wider African participation in international frameworks such as Council of Europe Convention 108, exactly the kind of cross-border enforcement capability the Malabo Convention's silence on inter-authority cooperation currently leaves untested. The Network is a more realistic vehicle for this than a new AU secretariat function would be, turning isolated national enforcement wins such as the Worldcoin case into a genuinely continental enforcement practice — provided it receives sustained funding, not intermittent capacity-building workshops.⁷⁴

7.4 Regional economic communities as the intermediate harmonisation layer

Regional economic communities, ECOWAS in particular, have a comparative advantage the AU level lacks: the ECOWAS Supplementary Act on Personal Data Protection is directly binding on member states without requiring separate national ratification, a stronger legal mechanism than the Malabo Convention's ratification-dependent model.⁷⁵

That binding character has not, on its own, guaranteed uniform enforcement, as the divergent pace of Nigeria and Ghana's implementation in Part 4 illustrates, despite both being ECOWAS members subject to the same Supplementary Act. Capacity gaps remain significant, and ECOWAS is currently undertaking a formal revision of the Supplementary Act to bring it into line with more recent developments in cross-border data transfer practice and data protection authority cooperation. That ongoing revision is a genuine opportunity: it should be used specifically to close the cross-border data flow gap identified in Part 2, instead of merely

⁷³Smart Africa and NADPA Signed an MOU to Advance the Enforcement and Harmonization of Personal Data Protection Laws in Africa' (Smart Africa, 10 March 2022) <<https://smartafrica.org/smart-africa-and-nadpa-signed-an-mou-to-advance-the-enforcement-and-harmonization-of-personal-data-protection-laws-in-africa/>> accessed 25 August 2026.

⁷⁴'Kenya's Data Protection Commissioner Calls for Stronger African Cooperation at NADPA Conference in Abidjan' (Tech Review Africa, 23 May 2026) <<https://techreviewafrica.com/news/5573/kenyas-data-protection-commissioner-calls-for-stronger-african-cooperation-at-nadpa-conference-in-abidjan>> accessed 23 August 2026.

⁷⁵Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (16 February 2010) <<https://africanlii.org/akn/aa-ecowas/act/2010/1-1/eng@2010-12-31>> accessed 28 August 2026.

updating the Supplementary Act's own definitions in isolation, so that West Africa's binding regional instrument does not inherit the same silence on cross-border flows that has weakened its continental counterpart.⁷⁶

7.5 Reconciling the security and trade tracks before they diverge further

Finally, the AU Commission and the AfCFTA Secretariat should establish a joint reconciliation process between the data governance provisions of the Digital Trade Protocol and the Malabo Convention before the two tracks harden into obligations that cannot be reconciled. Part 6 identified a real risk that the Protocol's cross-border data flow disciplines could, on the criticism levelled by Research ICT Africa and Afronomicslaw, favour established international platforms over the more protective approach reflected in the AU's own Data Policy Framework. Left unaddressed, this is not a marginal drafting inconsistency: it is two AU-endorsed continental instruments pulling African data governance in different directions, one prioritising human rights and security oversight, the other prioritising market access. A formal reconciliation mechanism, reporting jointly to the AU Commission and the AfCFTA Secretariat, is a more realistic near-term step than expecting either track to simply defer to the other.

8. Conclusion

This paper set out to test whether Africa's continental and national data governance instruments add up to a coherent roadmap for digital security, or merely a patchwork of overlapping obligations. The evidence assembled across Parts 2 to 6 supports the second reading more than the first, though not for want of ambition in any single instrument. The Malabo Convention took nine years to enter into force and, on the evidence in Part 2, still covers under a third of the continent's states nearly three years later, with two of its most digitally significant non-ratifying states, Nigeria and Algeria, sitting uncomfortably alongside their own leadership on global cybercrime diplomacy. The AU Continental AI Strategy, barely two years into a five-year implementation horizon, already displays the same geographic concentration that has long characterised Africa's digital economy more broadly, with the bulk of measured AI investment activity landing in four of the six states surveyed in Part 4. The six-country survey in Part 4

⁷⁶AUDA-NEPAD, 'Revision of the Supplementary Act A/SA.1/01/10 on the Protection of Personal Data in the ECOWAS Region' (Continental Engagement Platform) <<https://beta-citizenengagement.nepad.org/engagement/revision-of-the-supplementary-act-asa10110-on-the-protection-of-personal-data-in-the-ecowas-region>> accessed 28 August 2026.

showed that national law is not simply lagging behind these continental instruments; it is moving at four distinct speeds, from Kenya's assertive, court-tested enforcement against Worldcoin to Egypt's six-year gap between statute and operational enforcement machinery. Part 5 showed that consumer protection regulators, not only dedicated data protection authorities, are already doing meaningful data governance work on the ground in Nigeria's digital lending sector. Part 6 showed that the AfCFTA Digital Trade Protocol risks pulling data governance in a different direction from the Malabo Convention entirely, through provisions that critics argue favour established international platforms over the AU's own protective policy framework.

None of this is a reason to treat data privacy and consumer protection law as a secondary, technical concern to be resolved once the larger questions of military capability and economic policy have been settled. If anything, the relationship runs the other way. Personal data is the raw material both of the AI-driven security intelligence the continent is beginning to build and of the economic forecasting tools meant to buffer African economies against future shocks. A legal architecture that fails to govern that raw material coherently will produce brittle security tools and untrustworthy economic ones, regardless of how sophisticated the technology layered on top of it becomes. The five recommendations in Part 7, a model data protection law, an explicit institutional bridge between Malabo and the AI Strategy, a properly funded Network of African Data Protection Authorities, a reconciliation process between the ECOWAS and Malabo tracks, and a formal mechanism to align the Malabo Convention with the AfCFTA Digital Trade Protocol, are not offered as a comprehensive solution. They are offered as the minimum institutional plumbing needed before Africa's digital security ambitions and its digital trade ambitions stop working at cross purposes. Digital security, on this reading, is not a constraint on Africa's growth and stability. It is a precondition for both, and the continent's legal architecture has not yet caught up with that fact.

References

Treaties and Continental Instruments

1. African Union, African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, entered into force 8 June 2023)
2. African Union, Continental Artificial Intelligence Strategy (July 2024)
3. African Continental Free Trade Area, Protocol on Digital Trade (adopted February 2024)
4. Economic Community of West African States, Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (16 February 2010)

National Legislation

1. Nigeria Data Protection Act 2023
2. Federal Competition and Consumer Protection Act 2018 (Nigeria)
3. Protection of Personal Information Act 4 of 2013 (South Africa)
4. Data Protection Act No 24 of 2019 (Kenya)
5. Law No 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (Rwanda)
6. Data Protection Act 2012 (Act 843) (Ghana)
7. Law No 151 of 2020 Promulgating the Personal Data Protection Law (Egypt)

Secondary Sources

1. 'Accession to the Malabo Convention and the Future of Data Governance in Kenya' (Vellum Kenya, 1 October 2025) <<https://vellum.co.ke/accession-to-the-malabo-convention-and-the-future-of-data-governance-in-kenya/>> accessed 7 August 2026.
2. African Union, 'Africa Declares AI a Strategic Priority as High-Level Dialogue Calls for Investment, Inclusion, and Innovation' (au.int, 17 May 2025) <<https://au.int/en/pressreleases/20250517/africa-declares-ai-strategic-priority-investment-inclusion-and-innovation>> accessed 13 August 2026.

3. African Union, 'African Union Convention on Cyber Security and Personal Data Protection' (au.int) <<https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>> accessed 7 August 2026.
4. African Union, 'Continental Artificial Intelligence Strategy' (au.int, 2024) <<https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>> accessed 7 August 2026.
5. 'AI Policy Corner: AI and Security in Africa: Assessing the African Union's Continental AI Strategy' (Montreal AI Ethics Institute, 26 May 2026) <<https://montrealethics.ai/ai-policy-corner-ai-and-security-in-africa-assessing-the-african-unions-continental-ai-strategy/>> accessed 10 August 2026.
6. 'AI Policy Corner: AI and Security in Africa: Assessing the African Union's Continental AI Strategy' (Montreal AI Ethics Institute, 26 May 2026) <<https://montrealethics.ai/ai-policy-corner-ai-and-security-in-africa-assessing-the-african-unions-continental-ai-strategy/>> accessed 11 August 2026.
7. ALT Advisory, 'Malabo Convention Set to Enter Force' (dataprotection.africa, 19 May 2023) <<https://dataprotection.africa/malabo-convention-set-to-enter-force/>> accessed 7 August 2026.
8. ALT Advisory, 'Malabo Convention Set to Enter Force' (dataprotection.africa, 19 May 2023) <<https://dataprotection.africa/malabo-convention-set-to-enter-force/>> accessed 28 August 2026.
9. ALT Advisory, 'The Malabo Roadmap: Approaches to Promote Data Protection' (dataprotection.africa, September 2022) <https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf> accessed 9 August 2026.
10. ALT Advisory, 'The Malabo Roadmap: Approaches to Promote Data Protection' (dataprotection.africa, September 2022) <https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf> accessed 9 August 2026.
11. ALT Advisory, 'The Malabo Roadmap: Approaches to Promote Data Protection' (dataprotection.africa, September 2022) <https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf> accessed 6 August 2026.

12. 'Ambition or Inability: Assessing the African Union's Efforts to Establish AI Governance' (Future Center, 23 December 2025) <<https://futureuae.com/en-US/Mainpage/Item/10684/ambition-or-inability-assessing-the-african-unions-efforts-to-establish-ai-governance>> accessed 14 August 2026.
13. 'An Overview of Nigeria's Data Protection Act, 2023' (Securiti.ai) <<https://securiti.ai/overview-of-nigeria-data-protection-act/>> accessed 15 August 2026.
14. 'Analysis of FCCPC's Limited Interim Regulatory and Registration Framework and Guidelines for Digital Lending in Nigeria' (Lexology, 29 November 2022) <<https://www.lexology.com/library/detail.aspx?g=84f91798-86d1-4b3b-b092-f4d88dec68fc>> accessed 27 August 2026.
15. Andersen Egypt, 'Translation of Law No. 151 of 2020' <<https://eg.andersen.com/translation-law-151-2020/>> accessed 20 August 2026.
16. Andrew Gakiria and Tevin Mwenda Gitonga, 'What is the Malabo Convention?' (Diplo, 2025) <<https://www.diplomacy.edu/blog/what-is-the-malabo-convention/>> accessed 7 August 2026.
17. 'AU Strategy Guides AI Use as Technology Grows' (Africa Defense Forum, 5 August 2025) <<https://adf-magazine.com/2025/08/au-strategy-guides-ai-use-as-technology-grows/>> accessed 8 August 2026.
18. AUDA-NEPAD, 'Revision of the Supplementary Act A/SA.1/01/10 on the Protection of Personal Data in the ECOWAS Region' (Continental Engagement Platform) <<https://beta-citizenengagement.nepad.org/engagement/revision-of-the-supplementary-act-asa10110-on-the-protection-of-personal-data-in-the-ecowas-region>> accessed 28 August 2026.
19. Baker McKenzie, 'Egypt: Important Data Protection Update' (Baker McKenzie Insight, January 2026) <<https://www.bakermckenzie.com/en/insight/publications/2026/01/egypt-important-data-protection-update>> accessed 25 August 2026.
20. Baker McKenzie, 'Regulators, Enforcement Priorities and Penalties: South Africa' (Global Data and Cyber Handbook) <<https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/emea/south-africa/topics/regulators-enforcement-priorities-and-penalties>> accessed 18 August 2026.

21. Brenda Mwale, 'AI and Counter-Terrorism in Africa: Assessing the Role of the African Union's Continental AI Strategy' (GNET, 26 June 2025) <<https://gnet-research.org/2025/06/26/ai-and-counter-terrorism-in-africa-assessing-the-role-of-the-african-unions-continental-ai-strategy/>> accessed 8 August 2026.
22. Brenda Mwale, 'AI and Counter-Terrorism in Africa: Assessing the Role of the African Union's Continental AI Strategy' (GNET, 26 June 2025) <<https://gnet-research.org/2025/06/26/ai-and-counter-terrorism-in-africa-assessing-the-role-of-the-african-unions-continental-ai-strategy/>> accessed 10 August 2026.
23. Chatham House, 'The AU Can Help African Countries Adopt the UN Cybercrime Convention. But the Challenges Are Significant' (Chatham House, 31 October 2025) <<https://www.chathamhouse.org/2025/10/au-can-help-african-countries-adopt-un-cybercrime-convention-challenges-are-significant>> accessed 6 August 2026.
24. 'Data Protection Act, 2012 (Act 843) - Ghana' (Regulations.AI) <<https://regulations.ai/regulations/RAI-GH-NA-ACT8430-2012>> accessed 17 August 2026.
25. 'Data Protection Act, 2012' (Wikipedia) <https://en.wikipedia.org/wiki/Data_Protection_Act,_2012> accessed 17 August 2026.
26. 'Data Protection Compliance in Ghana' (TEMPLARS Law, 10 May 2023) <https://www.templars-law.com/app/uploads/2023/05/Data-Protection-Compliance-in-Ghana_final.pdf> accessed 17 August 2026.
27. 'Data Protection Enforcement: Understanding the Powers of Regulatory Authorities' (Lex Luminar, 24 June 2025) <<https://lexluminar.com/data-protection-enforcement-understanding-the-powers-of-regulatory-authorities/>> accessed 17 August 2026.
28. 'Economic Community of West African States' (CCDCOE) <<https://ccdcoe.org/organisations/ecowas/>> accessed 9 August 2026.
29. 'Egypt Data Privacy Laws: PDPL Law 151/2020 and the 2025 Executive Regulations' (Recording Law) <<https://www.recordinglaw.com/world-laws/world-data-privacy-laws/egypt-data-privacy-laws/>> accessed 25 August 2026.

30. 'Egypt Data Privacy Laws: PDPL Law 151/2020 and the 2025 Executive Regulations' (Recording Law) <<https://www.recordinglaw.com/world-laws/world-data-privacy-laws/egypt-data-privacy-laws/>> accessed 27 August 2026.
31. 'Egypt Data Protection Law' (PwC Middle East) <<https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/navigating-data-privacy-regulations/egypt-data-protection-law.html>> accessed 24 August 2026.
32. Federal Competition and Consumer Protection Commission, 'Registration of Digital Money Lenders' (fccpc.gov.ng) <<https://fccpc.gov.ng/registration-of-digital-money-lenders/>> accessed 27 August 2026.
33. 'From Aspiration to Implementation: The African Union AI Continental Strategy and the Development-Governance Paradox' (ResearchGate, 21 October 2025) <https://www.researchgate.net/publication/396230260_From_Aspiration_to_Implementation_The_African_Union_AI_Continental_Strategy_and_the_Development-Governance_Paradox> accessed 11 August 2026.
34. 'From Aspiration to Implementation: The African Union AI Continental Strategy and the Development-Governance Paradox' (ResearchGate, 21 October 2025) <https://www.researchgate.net/publication/396230260_From_Aspiration_to_Implementation_The_African_Union_AI_Continental_Strategy_and_the_Development-Governance_Paradox> accessed 17 August 2026.
35. Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (FPF, 18 November 2024) <<https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 8 August 2026.
36. Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (FPF, 18 November 2024) <<https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 10 August 2026.
37. Future of Privacy Forum, 'The African Union's Continental AI Strategy: Data Protection and Governance Laws Set to Play a Key Role in AI Regulation' (FPF, 18 November 2024)

- <<https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/>> accessed 8 August 2026.
38. 'Ghana's Data Protection Act 2012 (Act 843)' (ITLawCo, 28 January 2025) <<https://itlawco.com/focus-areas/data-protection-and-privacy/ghanas-data-protection-act-2012-act-843/>> accessed 18 August 2026.
 39. Jimena Sofia Viveros Alvarez, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade' (EJIL:Talk!, 14 June 2023) <<https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>> accessed 9 August 2026.
 40. Jimena Sofia Viveros Alvarez, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade' (EJIL:Talk!, 14 June 2023) <<https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>> accessed 10 August 2026.
 41. 'Kenya Data Protection Act 2019 (DPA) Compliance Guide' (Securiti) <<https://securiti.ai/kenya-data-protection-act-dpa/>> accessed 19 August 2026.
 42. 'Kenya: Data Protection Act Establishing Office of the Data Protection Commissioner Entered into Force' (Digital Policy Alert) <<https://digitalpolicyalert.org/event/27496-data-protection-act-2019-establishing-the-office-of-the-data-protection-commissioner-entered-into-force>> accessed 17 August 2026.
 43. 'Kenya's Data Protection Commissioner Calls for Stronger African Cooperation at NADPA Conference in Abidjan' (Tech Review Africa, 23 May 2026) <<https://techreviewafrica.com/news/5573/kenyas-data-protection-commissioner-calls-for-stronger-african-cooperation-at-nadpa-conference-in-abidjan>> accessed 23 August 2026.
 44. Law No 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (Rwanda) <<https://rwandalii.org/akn/rw/act/law/2021/58/eng@2021-10-15>> accessed 22 August 2026.
 45. 'Malabo Convention' (Wikipedia) <https://en.wikipedia.org/wiki/Malabo_Convention> accessed 13 August 2026.

46. 'Nigeria Data Protection Act 2023: Key Features and Legal Framework' (PlanetWeb Solutions) <<https://planetweb.ng/key-features-of-the-nigeria-data-protection-act-2023/>> accessed 17 August 2026.
47. 'Nigeria Data Protection Law: Complete NDPA Compliance Guide 2025' (Secure Privacy Blog) <<https://secureprivacy.ai/blog/nigeria-data-protection-law>> accessed 17 August 2026.
48. 'Nigeria's 2025 Consumer Lending Regulations: Key Frameworks and Guidelines' (SHQ Legal, 3 October 2025) <<https://www.shqlegal.com/publications/understanding-the-2025-digital-electronic-online-and-non-traditional-consumer-lending-regulations-in-nigeria>> accessed 27 August 2026.
49. 'Office of Data Protection Commissioner Finds WorldCoin Violated Data Protection Regulations' (JURIST, 26 October 2023) <<https://www.jurist.org/news/2023/10/office-of-data-protection-commissioner-finds-worldcoin-violated-data-protection-regulations/>> accessed 17 August 2026.
50. 'Office of Data Protection Commissioner Kenya: Compliance Guide' (Huduma Global Blog) <<https://hudumaglobal.com/blog/odpc-data-protection-act-kenya-compliance-guide>> accessed 17 August 2026.
51. Office of the Data Protection Commissioner v Tools for Humanity Corporation & 2 others (Worldcoin) Miscellaneous Criminal Application E315 of 2023; [2024] KEHC 312 (KLR) (Crim) (25 January 2024, Ruling) <<https://new.kenyalaw.org/akn/ke/judgment/kehc/2024/312/eng@2024-01-25>> accessed 18 August 2026.
52. Research ICT Africa, 'Alignment Problems: The AfCFTA Digital Trade Protocol and AI' (Just AI, 2025) <https://researchictafrica.net/wp-content/uploads/2025/02/Alignment-problems-AfCFTA-digital-trade-protocol-AI_Just_AI_2025.pdf> accessed 28 August 2026.
53. Research ICT Africa, 'Alignment Problems: The AfCFTA Digital Trade Protocol and AI' (Just AI, 2025) <https://researchictafrica.net/wp-content/uploads/2025/02/Alignment-problems-AfCFTA-digital-trade-protocol-AI_Just_AI_2025.pdf> accessed 27 August 2026.

54. 'Rwanda' (Data Protection Africa Fact Sheet) <<https://dataprotection.africa/rwanda/>> accessed 22 August 2026.
55. 'Rwanda Enacts Data Protection Law to Promote Rights to Privacy' (Paradigm Initiative, 5 December 2021) <<https://paradigmhq.org/rwandadataprivacy/>> accessed 23 August 2026.
56. 'Rwanda Enacts Data Protection Law to Promote Rights to Privacy' (Paradigm Initiative, 5 December 2021) <<https://paradigmhq.org/rwandadataprivacy/>> accessed 22 August 2026.
57. 'Safeguarding Privacy: South Africa's Protection of Personal Information Act (PoPIA)' (Infotrust, 5 September 2024) <<https://infotrust.com/articles/south-africas-protection-of-personal-information-act-popia/>> accessed 18 August 2026.
58. Shamaa Sheik, 'AU Convention on Cyber Security and Personal Data Protection | Malabo Convention' (Michalsons) <<https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281>> accessed 7 August 2026.
59. Shamaa Sheik, 'AU Convention on Cyber Security and Personal Data Protection | Malabo Convention' (Michalsons) <<https://www.michalsons.com/blog/au-convention-on-cyber-security-and-personal-data-protection-malabo-convention/65281>> accessed 9 August 2026.
60. 'Smart Africa and NADPA Signed an MOU to Advance the Enforcement and Harmonization of Personal Data Protection Laws in Africa' (Smart Africa, 10 March 2022) <<https://smartafrica.org/smart-africa-and-nadpa-signed-an-mou-to-advance-the-enforcement-and-harmonization-of-personal-data-protection-laws-in-africa/>> accessed 25 August 2026.
61. 'South Africa's Protection of Personal Information Act (POPIA) Explained' (Termly) <<https://termly.io/resources/articles/south-africas-protection-of-personal-information-act/>> accessed 19 August 2026.
62. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (16 February 2010) <<https://africanlii.org/akn/aa-ecowas/act/2010/1-1/eng@2010-12-31>> accessed 28 August 2026.

63. 'The AfCFTA's Digital Trade Rules Are Not Fit for Africa' (Afronomicslaw) <<https://www.afronomicslaw.org/category/analysis/afcftas-digital-trade-rules-are-not-fit-africa>> accessed 27 August 2026.
64. 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade' (Academia.edu) <https://www.academia.edu/103386834/The_African_Union_s_Malabo_Convention_on_Cyber_Security_and_Personal_Data_Protection_enters_into_force_nearly_after_a_decade_What_does_it_mean_for_Data_Privacy_in_Africa_or_beyond> accessed 6 August 2026.
65. 'The AU Continental AI Strategy: Concrete Safety Proposals or High-Tech Hype?' (Ilin Program) <<https://www.ilinaprogram.org/blog/au-continental-ai-strategy-2024>> accessed 11 August 2026.
66. 'The FCCPC's Limited Interim Regulatory/Registration Framework and Guidelines for Digital Lending, 2022' (Mondaq, 7 October 2022) <<https://www.mondaq.com/nigeria/dodd-frank-consumer-protection-act/1237972/the-fccpcs-limited-interim-regulatory-registration-framework-and-guidelines-for-digital-lending-2022>> accessed 27 August 2026.
67. 'The Global Majority in International AI Governance' (arXiv, 2025) <<https://arxiv.org/pdf/2601.17191>> accessed 10 August 2026.
68. 'The Malabo Convention: Africa's Cybersecurity and Data Protection Framework Explained' (African Researchers Magazine, 24 February 2025) <<https://www.africanresearchers.org/the-malabo-convention-africas-cybersecurity-and-data-protection-framework-explained/>> accessed 27 August 2026.
69. 'The Protection of Personal Information Act (POPIA): A Comprehensive Guide' (Captain Compliance) <<https://captaincompliance.com/education/the-protection-of-personal-information-act-popia-a-comprehensive-guide-to-south-africas-data-privacy-regulation/>> accessed 17 August 2026.
70. 'Toward an African Agenda for AI Safety' (arXiv, 2025) <<https://arxiv.org/pdf/2508.13179>> accessed 10 August 2026.

71. tralac Trade Law Centre, 'The OECD's New Index of Digital Trade Integration Shows Strong Gains from the AfCFTA's Digital Trade Protocol' (tralac, 2026) <<https://www.tralac.org/blog/article/16912-the-oecd-s-new-index-of-digital-trade-integration-shows-strong-gains-from-the-afcfta-s-digital-trade-protocol.html>> accessed 27 August 2026.
72. 'Understanding the Nigeria Data Protection Act, 2023 (NDPA)' (Cookie Script) <<https://cookie-script.com/privacy-laws/nigeria-data-protection-act-2023>> accessed 15 August 2026.
73. 'When Yes Means No – A Look at Kenya's Evolving Data Protection Framework' (Afriwise Insights) <<https://insights.afriwise.com/blog/when-yes-means-no-a-look-at-kenyas-evolving-data-protection-framework>> accessed 18 August 2026.
74. 'Who We Are' (Data Protection & Privacy Office, Rwanda) <<https://dpo.gov.rw/about-us/who-we-are>> accessed 23 August 2026.
75. 'Worldcoin Case a \'Watershed Moment\' for Data Protection in Kenya' (IAPP, 28 May 2026) <<https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya>> accessed 17 August 2026.
76. 'Worldcoin: Intrigues of Data Privacy' (Daily Nation, 1 December 2025) <<https://nation.africa/kenya/news/worldcoin-intrigues-of-data-privacy--5282596>> accessed 19 August 2026.