

The background image features a glowing map of Africa composed of white circuit lines and red dots. A large, thick red prohibition symbol (a circle with a diagonal slash) is overlaid on the map. A human hand is shown from the right, with the index finger pointing towards the center of the map, where it appears to be touching or activating a point of light. The overall color scheme is dark with blue and red highlights.

Governing Artificial Intelligence in Africa: A Principles-based Framework for Responsible Regulation



Notice

This paper was prepared by Vodacom Group Limited (“Vodacom”) under the mandate agreed between Vodacom and its service providers. It is intended to help regulators and policymakers across Africa understand international and regional regulatory and policy developments concerning AI tools, products and services, including the treatment of data and infrastructure, and to identify gaps and opportunities in local laws, regulations and policies that may support responsible AI innovation.

Vodacom and its service providers accept no responsibility or liability to any party for this paper or its contents. The paper must not be used for any other purpose or context. Its facts, statements, views and suggestions are based on research and analysis conducted within the agreed scope, limits and context of the mandate. The content is generally accurate only as at the date on which the research was finalised, being October 2026.

Use of this report

All copyright and other intellectual property rights in the report remain the property of Vodacom. To the fullest extent permitted, Vodacom disclaims liability arising from the use of the report or its contents, including any action or decision taken in reliance on them.

Vodacom Group Limited

Executive summary

This paper sets out **Vodacom's recommended approach** to **artificial intelligence** governance in Africa. AI is being deployed across the continent at accelerating speed, yet the steps towards the development of regulatory frameworks needed to manage its risks and realise its benefits remain uneven across African jurisdictions.

Vodacom submits that AI governance in Africa should not simply replicate any single international model. While international frameworks provide valuable lessons, effective governance must be adapted to Africa's infrastructure constraints, institutional capacity, data governance challenges, digital literacy disparities and broader socio-economic realities, while enabling African countries to participate meaningfully in the development, deployment, and governance of AI technologies.

Ayman Essam
Group Chief Officer:
External Affairs



Executive summary

continued

Accordingly, Vodacom proposes an AI governance framework founded on the protection and promotion of human rights, fundamental freedoms, and human dignity throughout the AI lifecycle. It operationalises this foundation through six governance principles: (1) transparency and explainability; (2) accountability and human oversight; (3) fairness and non-discrimination; (4) safety and security; (5) privacy and data protection; and (6) proportionality.

Vodacom strongly recommends a common horizontal governance baseline, implemented through a hybrid institutional model that combines central coordination with sector-specific oversight, supported by graduated oversight mechanisms and phased implementation pathways aligned with differing levels of regulatory maturity.

Vodacom recognises the cross-border nature of AI systems, data flows and digital infrastructure, and the resulting importance of regional harmonisation, regulatory cooperation, and strong regional economic communities in promoting policy alignment, interoperability, and regional digital market integration. These recommendations are offered as a constructive contribution to the development of practical, rights-respecting and context-sensitive AI governance frameworks across Africa, consistent with the objectives of the African Union's Continental Artificial Intelligence Strategy, 2024.



Introduction

Artificial intelligence (AI) is rapidly becoming a foundational technology **with the potential to transform economies, public services, and societies.**

Across a myriad of sectors, AI systems are already being deployed to improve efficiency, enhance decision-making, and expand access to services. The policy debate is no longer whether AI should be governed, but how to develop governance frameworks that promote innovation, protect individuals, and support inclusive economic growth.

In its Continental Artificial Intelligence Strategy, 2024 (the **AU AI Strategy**), the African Union (**AU**) characterises AI as “a driving force for positive change, socio-economic transformation and cultural renaissance”.¹ Africa has a young and rapidly growing population,² an expanding digital economy,³ increasing levels of connectivity,⁴ and globally recognised leadership in mobile-based innovation.⁵ AI is projected to contribute up to \$1.5-trillion to Africa’s economy by 2030.⁶ But the potential of AI in Africa exceeds economic gains;⁷ AI systems are also performing critical functions in key developmental sectors such as healthcare,⁸ agriculture,⁹ financial services,¹⁰ and public administration.¹¹

Realising these opportunities requires Africa to become an active participant in the AI economy: developing, shaping, and owning AI systems that reflect African languages, needs, and priorities, rather than remaining a consumer of systems designed by and for other regions.¹² It equally requires that access to AI technologies and their benefits extends to all, including rural, low-income, and other underserved and marginalised communities, so that AI narrows rather than widens existing digital divides.¹³

While AI presents transformative opportunities, it also gives rise to significant risks. Emerging concerns include the potential for discrimination and bias in automated decision-making, privacy infringements, misinformation, intellectual property infringements, cybersecurity threats, lack of transparency, labour market disruption, and the concentration of market power among a small number of firms.¹⁴



Introduction

continued

Many of these risks will manifest differently, and in some cases more acutely, within African contexts. For example, the availability of representative local datasets remains limited, increasing the risk that AI systems trained primarily on foreign data produce inaccurate or discriminatory outcomes when deployed in African markets.¹⁵ Uneven levels of digital literacy, gaps in infrastructure, linguistic diversity, and varying levels of institutional capacity may also affect the ability of individuals to understand, challenge, or obtain remedies for AI-enabled decisions.¹⁶

Effective AI governance in Africa must therefore pursue two complementary objectives: enabling innovation, economic opportunity, and access, while safeguarding human dignity, fundamental rights, and democratic values. These objectives are not in tension: predictable, principled, and proportionate governance can reduce uncertainty for innovators and build public trust on which AI adoption depends.¹⁷

However, for African countries, the need for effective governance is further complicated by the increasingly cross-border nature of the digital economy. AI systems, data flows, cloud services, and telecommunications infrastructure frequently operate across multiple jurisdictions, creating the risk of regulatory fragmentation and inconsistent standards. Greater regional alignment will therefore be essential to promote legal certainty, facilitate innovation, and support effective oversight.

Accordingly, this paper argues that African countries should pursue a pragmatic, risk-based and context-sensitive approach to AI governance that simultaneously promotes innovation, economic development, and public trust while safeguarding fundamental rights. Drawing on international experience and emerging African initiatives, it proposes a governance framework grounded in human rights principles that is responsive to local realities, capable of supporting responsible AI adoption, and sufficiently flexible to accommodate future technological developments. The principles, institutional architecture, and oversight mechanisms proposed in this paper should be read together as a framework for preventing such harms and providing effective remedies where harms do occur.

Vodacom, as a pan-African telecommunications operator that deploys AI systems across multiple jurisdictions, has direct operational experience of the practical challenges that arise where governance frameworks are absent, fragmented,

or poorly calibrated. Vodacom acknowledges that, as both a deployer of AI systems and a proponent of enabling governance reform, it occupies a dual role that warrants transparency. The recommendations in this paper are therefore informed by Vodacom's experience in markets characterised by infrastructure and resource constraints, regulatory fragmentation, and diverse consumer needs, and are offered in the spirit of constructive partnership with policymakers and regulators, rather than as a substitute for independent regulatory judgment. This approach is consistent with the AU AI Strategy, which recognises the private sector as an important stakeholder in AI governance and implementation, with a role to play in identifying emerging challenges, contributing technical expertise, supporting capacity-building, and developing practical solutions in partnership with governments, regulators and international organisations.¹⁸



Learning from global AI governance frameworks

Any credible African AI governance framework must engage with the principal international reference points.¹⁹ **The purpose is not to adopt these instruments wholesale, but to extract best practice and transferable elements,** and identify where fundamental adaptation is required.

Indeed, the AU AI Strategy recommends that African countries “develop flexible and adaptable AI regulation and legislation models by drawing on global and regional experiences” which are then adapted “to their settings and needs”²⁰ The analysis below begins by identifying the points of convergence across these frameworks before examining the specific models that have been adopted and their applicability to African contexts.

Emerging global consensus

Although regulatory approaches differ across jurisdictions, a degree of international consensus is beginning to emerge around foundational principles for AI governance. The OECD’s Recommendation on Artificial Intelligence (which establishes the OECD AI Principles),²¹ the UNESCO Recommendation on the Ethics of Artificial Intelligence (the **UNESCO Recommendation**)²², the G7 Hiroshima AI Process,²³ the Council of Europe Framework Convention on Artificial Intelligence (the **European Framework Convention**)²⁴, and the US National Institute of Standards and Technology’s Artificial Intelligence Risk Management Framework (the **NIST Framework**)²⁵ all position themselves as primarily human rights-respecting frameworks, which emphasise concepts such as human-centred development, transparency and explainability, accountability, fairness, security and safety, privacy protection, and human oversight.²⁶ The AU AI Strategy similarly captures these concepts as “guiding principles”, reflecting broad alignment between African and international thinking on the fundamental objectives of AI governance.²⁷ This convergence suggests that African policymakers do not need to reinvent AI governance from first principles. The more difficult question concerns how those principles should be operationalised.



Learning from global AI governance frameworks

continued

The value and limits of the European approach



The most comprehensive AI regulatory framework currently in force is the European Union's AI Act (the **EU AI Act**),²⁸ which adopts a risk-based approach to regulation. Under the EU AI Act, AI systems are classified into four tiers: (1) unacceptable risk, which is prohibited;²⁹ (2) high risk, which is subject to stringent compliance requirements,

including pre-deployment conformity assessments and post-market monitoring;³⁰ (3) limited risk, which is subject to transparency obligations;³¹ and (4) minimal risk, which are unregulated. Non-compliance may result in administrative fines of up to €35-million or 7% of the offending entity's global annual turnover, whichever is higher.³²

The risk-based structure of the EU regime offers an important lesson: regulatory obligations should be proportionate to the potential harms posed by AI systems. This avoids the inefficiencies of treating all AI applications in the same manner.

However, the EU approach embeds several structural assumptions that limit its direct applicability in many African jurisdictions. First, it presupposes the existence of conformity assessment bodies, market surveillance authorities, and other competent regulators with specialised expertise in AI, as well as the financial and human resources necessary to oversee its deployment and associated human rights and safety risks.³³ Second, compliance costs are significant, with initial estimates from the European Commission's own impact assessment ranging between €6,000 – €7,000 per AI application developed.³⁴ The European Commission acknowledged that smaller firms would be disproportionately affected because their capacity to absorb such burdens is much more limited.³⁵ Imposing European-scale compliance burdens in an African jurisdiction could stifle innovation, price out emerging African developers, and delay equitable access to locally relevant AI. Relatedly, the EU AI Act's framework is tailored to European market structures and fundamental rights jurisprudence, and does not fully account for the realities of many African contexts, including informal economies, digital literacy disparities, and linguistic diversity.³⁶ Accordingly, while the EU model's risk-based approach offers valuable guidance, the specific regulatory architecture through which that approach is implemented may not be readily transferable to Africa.

Alternatives to the European approach



The United Kingdom (**UK**) adopts a principles-based approach to AI governance that relies primarily on existing regulatory frameworks and sector-specific regulators, rather than the creation of AI-specific legislation or regulatory bodies.³⁷ To promote regulator coherence, the UK has developed a framework of cross-cutting principles, which are intended to guide the responses of regulators to AI-related risks and opportunities in their sectors, in accordance with existing laws and regulations that apply to their remits.³⁸ While the UK has considered imposing a statutory mandate on regulators to have due regard for the framework, their implementation currently remains within the discretion of individual regulators.³⁹ The model demonstrates how AI governance can be integrated into existing regulatory structures, thereby avoiding the institutional and resource burdens associated with establishing dedicated AI regulatory regimes.

However, the UK approach also depends on the existence of sufficiently mature and capable sectoral regulators with the technical expertise, resources, and institutional capacity to interpret and apply AI governance principles within their respective sectors – an assumption that cannot be made across all African jurisdictions. In addition, the UK approach is primarily concerned with the governance of AI risks within existing regulatory domains and does not seek to address broader structural issues associated with AI development and adoption, including access to data, compute infrastructure, and sustainability.⁴⁰ As discussed below, these issues are central to AI governance in many African jurisdictions and may therefore require a more comprehensive policy response than the UK framework presently contemplates.



Singapore's more pragmatic approach to AI governance is grounded in its National AI Strategy⁴¹ and supported by a suite of governance frameworks and guidance documents,⁴² rather than a comprehensive AI statute. Instead of imposing extensive binding legal requirements, Singapore developed detailed, practical guidance for private sector organisations, complemented by its AI Verify Testing Framework, which provides tools to assist organisations in translating AI governance principles into practice.⁴³

Learning from global AI governance frameworks

continued

The model is particularly relevant to African jurisdictions because it demonstrates that meaningful AI governance can be achieved through structured guidance, voluntary standards, and practical implementation tools, without the significant institutional and resource demands associated with a comprehensive regulatory regime. The approach is less resource-intensive than alternative models, but it also depends on a level of private sector sophistication and regulatory coordination that is inconsistent across the African continent.



China adopts a targeted approach to AI governance, regulating particular AI applications that are not already addressed by its general cybersecurity, data security, and data protection laws.⁴⁴ This approach includes dedicated rules for, among other things, algorithmic recommendation engines,⁴⁵ deepfake technologies,⁴⁶ and generative AI.⁴⁷

While China's highly centralised regulatory model may not be directly transferable to Africa's diverse political and institutional contexts, its strategy of regulating specific high-risk AI applications through targeted measures, rather than through a single comprehensive framework, offers another pragmatic approach for jurisdictions with limited regulatory capacity. Such an approach enables regulators to address the most pressing AI-related risks while avoiding the institutional and resource burdens associated with developing and enforcing a comprehensive AI regime.

Continental and regional reference points

While the international frameworks outlined above offer valuable principles and structural models, none are directly transposable to the African continent. By contrast, the AU AI Strategy provides Africa's own continental reference point, proposing a multi-tiered approach to AI governance in Africa comprising five activities: (1) amending existing laws; (2) identifying regulatory gaps; (3) establishing enabling policy frameworks; (4) developing AI assessment tools; and (5) conducting continuous research.⁴⁸ It also advocates for the establishment of independent institutions to conduct oversight on the use of AI, enforce compliance with standards as they emerge, and provide access to redress and remedy where violations occur.⁴⁹ Vodacom accepts and supports the AU AI Strategy's multi-tiered approach as the appropriate architecture for African AI governance, and the recommendations in this paper are designed to support its implementation.

At the regional level, AI is increasingly becoming a focus for Regional Economic Communities (**RECs**), which are well placed to translate continental objectives into more context-specific regional priorities and implementation mechanisms.⁵⁰ For instance, the Southern African Development Community (**SADC**) emphasises the development and implementation of national AI strategies tailored to local circumstances while drawing on international innovation and experience to advance the broader objectives of its digital transformation strategy.⁵¹ SADC further recommends the World Economic Forum's Framework for Developing a National Artificial Intelligence Strategy⁵² as a resource to support Member States in designing their own AI strategies. In addition to promoting greater policy alignment, SADC also envisages the development of a single regional digital market supported by interoperable digital systems and infrastructure.⁵³

Similarly, the East African Community (**EAC**) has adopted the EAC Declaration on Artificial Intelligence, which promotes responsible, ethical, and inclusive AI governance in the region through risk-based regulatory frameworks, strengthened transparency and accountability, alignment with international standards, and the integration of ethical and inclusivity principles across all AI systems.⁵⁴ The EAC's most recent development strategy further identifies digital transformation and the establishment of a regional AI programme as strategic priorities, with a particular focus on aligning national AI policies, promoting interoperable data systems across Member States, and piloting AI initiatives in priority sectors.⁵⁵ Together, these initiatives demonstrate the growing role of RECs in fostering regulatory coherence, interoperability and regional digital market integration as part of Africa's emerging AI governance architecture.

African realities that should shape AI governance

Having identified the transferable elements and limitations of international and regional approaches, **it is necessary to examine the specific structural conditions that will determine how any governance framework operates in African contexts.**⁵⁶ In this regard, Vodacom has identified **four interrelated factors** that define the African regulatory environment and impose constraints on governance design.

Infrastructure constraints

Africa accounts for only approximately one percent of global data centre capacity, with about 223 facilities across 38 countries.⁵⁷ The AU AI Strategy identifies limited internet access, inadequate computing infrastructure, insufficient data for training AI models, and a shortage of AI-related skills as key barriers to AI uptake.⁵⁸ In addition, unreliable electricity supply remains a persistent challenge in many countries, with organisations often relying on generators and uninterruptible power supply systems to maintain operations.⁵⁹ Connectivity constraints are also significant: in Mozambique, only 19.8% of the population has internet access.⁶⁰ In Tanzania, 5G coverage remains concentrated in urban areas, with only 900 base stations nationally as at December 2024.⁶¹ Even Kenya, one of Africa's digital leaders, has fibre-to-the-home coverage of just 13%,⁶² and lacks sufficient domestic compute capacity to support advanced AI workloads.⁶³ Given its limited capacity to develop, train, or host its own foundation models, Africa remains predominantly a consumer of AI systems developed elsewhere.

These deficits constrain both Africa's ability to build and commercialise its own AI systems, and equitable access to AI across communities. Research shows that mobile data costs up to 26% of household expenditure in some regions, and rural and low-income communities are least able to access AI-enabled services.⁶⁴



African realities that should shape AI governance

continued

Accordingly, any AI governance framework that assumes widespread high-speed connectivity and abundant computational resources is unlikely to be effectively implemented across much of the continent. Rather, the framework should actively support local AI research and development, incentivise investment in domestic compute and cloud infrastructure, promote the development of African-language datasets and contextually-appropriate AI applications, promote affordable and equitable access to connectivity, devices, compute, and AI-enabled services, and ensure that access to global AI systems does not create dependencies that undermine policy autonomy, data sovereignty, or economic resilience. Without affordable connectivity, reliable power, and local compute, African developers cannot become active participants in the AI economy, and underserved communities are less likely to gain equitable access to AI's benefits.⁶⁵ In other words, an African AI governance framework must sufficiently balance openness to global digital ecosystems with strategic investment in Africa's own AI capabilities.

Data governance

Africa faces significant data governance challenges. In the first instance, the continent's data governance framework remains fragmented. The AU Convention on Cyber Security and Personal Data Protection (the **Malabo Convention**),⁶⁶ which aims to provide a harmonised framework for cybersecurity and data protection across the continent, was initially adopted in 2014 but only came into effect in 2023 after having finally received the minimum 15 ratifications required to come into force.⁶⁷ To date, the Malabo Convention has been ratified by only 20 of the 55 AU Member States.⁶⁸ As a result, data protection and cybersecurity rules remain uneven across jurisdictions, creating uncertainty for organisations operating across borders, and increasing the compliance cost of cross-border data flows.

Second, as noted above, many African countries remain dependent on foreign digital infrastructure. The Kenya AI Policy, for instance, identifies reliance on foreign hyperscale cloud providers as a structural challenge, noting the concentration of global cloud infrastructure among a small number of providers.⁶⁹ This dependence limits domestic control over the storage and processing of data that underpin AI systems.

The solution, however, is not simply the imposition of blanket localisation requirements. Rather, African countries must balance openness with autonomy. That is, as African countries expand their AI capabilities, they must balance the need to retain meaningful

control over data generated by their populations, and the tools that process it, with the benefits of cross-border data flows supporting innovation and access to computing resources. This approach is endorsed by the AU's Data Policy Framework⁷⁰ and the Agreement Establishing the African Continental Free Trade Area (the **AfCFTA**).⁷¹

Africa's data governance challenges are not merely regulatory or operational in nature. Data governance frameworks play a critical role in protecting privacy, autonomy, and other fundamental rights. Significant divergences between national regimes may create uncertainty regarding the standards applicable to data processing activities and may result in differing levels of protection for individuals across jurisdictions.

AI governance in Africa should focus on strengthening and harmonising data governance frameworks, expanding domestic digital infrastructure, and developing privacy protective mechanisms for responsible cross-border data flows without resorting to blanket data localisation requirements.⁷²

Digital literacy disparities

The AU's Digital Transformation Strategy for Africa acknowledges that the continent's literacy rate is approximately 64%, compared to a global average of 86.3%.⁷³ The Kenya AI Policy identifies gaps in the public sector's capacity to procure, deploy, and oversee AI systems, noting that AI has not yet been systematically integrated into formal education curricula.⁷⁴ Similarly, the Tanzania AI Framework recognises low levels of digital literacy, particularly in rural areas, as a significant constraint on AI adoption.⁷⁵ Digital literacy gaps are also not experienced evenly: gender and intersecting forms of disadvantage, including disability, age, income, and language, can compound them, with women in Africa having lower adult literacy and access to digital technologies than men.⁷⁶

The challenge of digital literacy also has an important rights dimension. Transparency measures are only effective where individuals are able to understand when AI systems are being used, how decisions relating to AI may affect them, and what avenues exist to challenge or seek remedies for adverse outcomes. Building public awareness and digital literacy should therefore be viewed as an essential component of meaningful accountability.

African realities that should shape AI governance

continued

Existing inequalities and exclusion

Approximately 86% of Africa's workforce is employed in the informal sector.⁷⁷ AI-enabled credit-scoring and risk-assessment systems may therefore reinforce existing patterns of financial exclusion if they rely exclusively on data generated within formal economic systems. Similar concerns arise in relation to longstanding disparities between urban and rural communities, where unequal access to digital infrastructure, connectivity, public services, and economic opportunities may result in uneven participation in data-driven systems. Differences in literacy, educational attainment, digital skills, and language representation may further affect individuals' abilities to access, understand, challenge, or benefit from AI systems.

Regulatory frameworks that require AI systems to operate fairly are therefore required to define fairness with reference to populations that are often absent from conventional datasets and must ensure that fairness metrics developed in highly formalised or demographically homogenous environments are not applied uncritically in African contexts. This requires governance mechanisms to account for informal economic activity and other structural inequalities that shape participation in African societies and economies.

Particular attention should also be paid to the risk that AI systems may entrench or amplify existing social and economic inequalities. Biased training data, inadequate representation of African populations in datasets, and poorly designed decision-making systems may result in the exclusion or disadvantage of individuals and communities that are already marginalised, including women, youth, people with disabilities, those operating within informal economies, living in rural or underserved areas, or possessing lower levels of literacy and formal education.⁷⁸ Without intervention at the design, deployment, and oversight stages, such systems may replicate existing patterns of exclusion across financial services, employment opportunities, healthcare access, and public services, while projecting an appearance of neutrality. Addressing these risks is important not only for economic development and social inclusion, but also for ensuring that AI adoption reduces, rather than reinforces, existing inequalities, and for safeguarding the rights to equality and dignity.



A principles-based governance framework and its institutional architecture

Drawing on the international frameworks and the contextual realities documented above, **Vodacom recommends that African jurisdictions adopt an AI governance framework that is founded on respect for and protection and promotion of human rights, fundamental freedoms, and human dignity** throughout the AI lifecycle, such that AI systems provide new means to advocate for, defend, exercise, and fulfil human rights, rather than infringe them.⁷⁹

Vodacom recommends that any African AI governance framework operationalises this foundation through six principles, namely: (1) transparency and explainability; (2) accountability and human oversight; (3) fairness and non-discrimination; (4) safety and security; (5) privacy and data protection; and (6) proportionality. These principles are articulated in the UNESCO Recommendation, the OECD AI Principles, the NIST Framework, and the AU AI Strategy, and have been adopted by virtually every national framework reviewed, including the EU AI Act, and the approaches of the UK,⁸⁰ Egypt,⁸¹ Mauritius,⁸² Kenya,⁸³ Nigeria,⁸⁴ and Tanzania.⁸⁵ These principles should not be understood merely as ethical aspirations, but as practical governance mechanisms through which AI-related risks to human rights may be identified, mitigated and addressed.

This framework is directed, in particular, at AI systems that materially affect human rights. For such systems, the **six principles** set out below are intended to operate together as an integrated framework: transparency and explainability enable affected persons to know when and how AI has been used; fairness, safety, privacy, and proportionality define the standards against which AI systems are assessed; and accountability and human oversight provide the means to challenge, review, correct, and obtain redress for adverse outcomes.

Transparency and explainability

Transparency and explainability requirements should be adapted to African conditions. In light of the digital literacy disparities documented above, transparency should be operationalised through layered mechanisms, including plain-language disclosures for end users in local languages, structured technical disclosures for sector regulators, and comprehensive technical documentation for expert auditors. Individuals affected by significant AI-enabled decisions should be able to understand, at an appropriate level, how AI systems are being used and the principal factors that influenced those decisions.

Accountability and human oversight

Accountability frameworks should clearly allocate responsibility at each stage of the AI lifecycle, including among providers, deployers, and users. Organisations should be required to identify, prevent, mitigate, monitor and account for actual and potential AI-related impacts on rights, including through proportionate human rights impact assessments, stakeholder engagement, accessible complaints mechanisms and remediation pathways for affected individuals and communities.⁸⁶ Where an AI system materially affects fundamental rights, affected individuals should be entitled to an explanation, human review, and an effective remedy. Human oversight should be capable of overriding, revising, or reversing an AI-assisted decision where necessary.⁸⁷ Effective accountability arrangements should also provide accessible routes to explanation, challenge, correction, and redress, including non-digital mechanisms for communities with limited connectivity.

Fairness and non-discrimination

Fairness metrics must incorporate proxy measures for populations outside formal data systems, and impact assessments must evaluate whether AI systems entrench or alleviate exclusion in credit, healthcare, education, and public service delivery. Fairness should be understood not only as a technical objective but also as a governance imperative aimed at preventing discrimination and promoting equal treatment. Organisations should take reasonable steps to identify, assess and mitigate potential biases throughout the development and deployment of AI systems, particularly where those systems may affect access to opportunities, services or rights.

A principles-based governance framework and its institutional architecture

continued

Safety and security

AI systems should be designed, deployed and operated in a manner that is safe, secure, reliable and resilient throughout their lifecycle. AI governance frameworks should require appropriate measures to manage risks arising from system failures, inaccurate outputs, malicious interference, cybersecurity threats and misuse.⁸⁸ In the African context, these measures should also address AI-enabled threats to democratic processes, social cohesion and fundamental rights, including misinformation, disinformation, hate speech, technology-facilitated gender-based violence and unlawful surveillance. Given existing infrastructure constraints, governance frameworks should further promote resilience and appropriate safeguards against service disruption.

Privacy and data protection

The development and deployment of AI systems should be consistent with applicable privacy and data protection requirements. Governance frameworks should promote responsible data collection, processing, storage, sharing and retention practices, while ensuring that individuals retain appropriate protections against unlawful, excessive or disproportionate uses of personal information.

Proportionality

Regulatory obligations should be proportionate to the nature, likelihood, and severity of the risks posed by an AI system. Governance frameworks should therefore distinguish between low-risk and high-risk applications, concentrating regulatory resources where the potential for harm is greatest. This also reduces the risk that excessive compliance burdens may be imposed on small and medium-sized enterprises and emerging sectors, thereby stifling innovation and undermining African participation in the AI economy.⁸⁹ Risk classifications should be adapted to local conditions and societal contexts rather than transplanted directly from highly formalised economies.⁹⁰ For instance, an AI-enabled credit scoring system operating in a context where 85% of the workforce is informal should be classified differently than the same system in a formalised European economy, because the potential for exclusionary harm is materially higher.



A principles-based governance framework and its institutional architecture

continued

Institutional design

Vodacom's preferred approach for giving concrete effect to these principles is a horizontal approach drawing on elements of the EU AI Act, which establishes a common baseline that is supplemented by targeted sector-specific measures where necessary. This baseline should establish common principles, terminology, risk-classification criteria, transparency obligations, accountability standards, and rights-based safeguards across the economy, while allowing sector regulators to issue tailored guidance or requirements where sector-specific risks cannot be adequately addressed through the common framework.

Regarding institutional bodies, three models are available: a standalone AI regulatory agency, an embedded function within existing regulators (for example, the telecommunications regulator or data protection regulator), and a multi-stakeholder governance council. A standalone agency offers a dedicated mandate but requires substantial resources that most African jurisdictions cannot currently commit.⁹¹ An embedded function leverages established institutional capacity but risks fragmented oversight where AI applications cut across sectoral boundaries. A multi-stakeholder council provides advisory and coordination functions but may lack enforcement authority. The experience of African countries already implementing AI governance suggests that distributing functions across multiple agencies creates risks of *"divergent priorities, internal conflicts, power struggles, and regulatory fragmentation"*.⁹²

Vodacom therefore recommends a hybrid approach, adaptable to national contexts and priorities, that combines central coordination with sector-specific oversight. This approach would entail governments designating a lead coordination body (ideally within an existing ministry or regulatory authority with digital and data governance mandates and expertise) to provide overarching direction and coherence for AI governance. Existing sector regulators would retain responsibility for regulating and enforcing AI-related obligations within their domains, while a multi-stakeholder advisory council would provide technical expertise and stakeholder input. This model avoids standalone agencies that exceed current resource capacities, and builds on existing institutional mandates, where possible.⁹³

The effectiveness of this model will depend on clearly defining the lead body's mandate, accountability mechanisms, and relationship with sector regulators. In particular, Vodacom's recommended approach incorporates the following elements:⁹⁴

Legal mandate: The lead coordination body should be established or empowered by legislation or, in the interim, an appropriate executive instrument, to develop cross-sectoral AI standards, coordinate sector regulators, and exercise limited direct oversight of issues that extend beyond the mandate of any single sector regulator. As far as possible, the lead coordination body should not derogate from the statutory powers and functions of sector regulators.

Accountability: The lead coordination body should operate transparently and be subject to appropriate accountability mechanisms, including annual reporting to Parliament, public consultation on proposed standards and guidance, and judicial review of its decisions. Sector regulators should remain accountable through their existing statutory governance and oversight frameworks when applying and enforcing AI-related requirements within their respective sectors.

Decision-making authority: The lead coordination body should be responsible for issuing general AI standards, principles and risk-classification criteria applicable across sectors. Sector regulators should apply and enforce those standards within their respective domains. The lead body should exercise direct authority only where an issue is cross-sectoral and cannot be effectively addressed by a single regulator, where no sector regulator has competence over the issue, or where a material dispute arises between sector regulators.

On oversight mechanisms, Vodacom recommends a graduated menu calibrated to each jurisdiction's institutional capacity. These oversight mechanisms should be designed to identify and mitigate rights-related harms before and after deployment, and to ensure that affected individuals have practical routes to explanation, challenge, correction, and redress. In practice, non-digital routes may include community-based complaint mechanisms, mobile-based reporting channels, local language help desks, and referrals to traditional dispute resolution bodies, particularly where connectivity, literacy, or institutional access is limited.

A principles-based governance framework and its institutional architecture

continued

At the foundation level, all jurisdictions should require providers of high-risk AI systems to maintain documentation of system design, training data, and performance metrics. **At the intermediate level**, jurisdictions with functional data protection authorities should introduce mandatory impact assessments prior to deployment for AI systems that affect fundamental rights or access to essential services, drawing on UNESCO's Ethical Impact Assessment methodology,⁹⁵ which has been endorsed by the AU AI Strategy.⁹⁶ These assessments should evaluate risks relating to fairness, privacy, safety, discrimination, security, transparency, and broader societal impacts, and should identify appropriate mitigation measures as a condition of deployment. **At the advanced level**, jurisdictions with mature institutional capacity should establish algorithmic auditing functions, public registries for high-risk AI systems, and incident reporting obligations. Regulatory sandboxes should be deployed across **all maturity levels**, as endorsed by the AU AI Strategy,⁹⁷ and reflected in Kenya,⁹⁸ Mozambique,⁹⁹ and Egypt.¹⁰⁰



A phased roadmap for AI governance in Africa

The phased roadmap below operationalises the principles and institutional architecture described above by sequencing obligations as institutional capacity matures.

African countries are entering the AI era from markedly different starting points. A one-size-fits-all implementation model is unlikely to succeed. Rather than attempting to immediately replicate the comprehensive regulatory frameworks emerging in more mature digital economies, African governments should adopt a phased approach.

1

2

3

Phase One | Establishing governance foundations

The priority is to adopt a national AI strategy aligned with the AU AI Strategy, to enact or strengthen existing legislation, to designate a lead coordination body, and to establish basic transparency requirements for high-risk AI systems, including systems used to determine access to essential services (such as credit, insurance, healthcare, education, and employment), as well as biometric identification and surveillance technologies.¹⁰¹ In many jurisdictions, strengthening existing legal frameworks relating to data protection, cybersecurity, consumer protection, intellectual property, competition regulation, telecommunications regulation, and digital governance may provide more immediate governance benefits than developing standalone AI legislation.¹⁰²

Concrete triggers for transitioning to Phase Two should include: (1) the establishment of a functional Data Protection Authority with enforcement capacity; (2) the adoption of a national AI strategy with budgetary allocations; and (3) the completion of at least one regulatory capacity-building programme for staff of oversight institutions.

Phase Two | Implementing risk-based governance mechanisms

Once foundational governance structures are established, governments can introduce targeted regulatory measures focused on higher-risk uses of AI. This includes introducing mandatory AI impact assessments for high-risk systems, developing sector-specific guidance for telecommunications, financial services, healthcare, education, employment, public administration, and digital platforms, establishing regulatory sandboxes, and developing incident reporting mechanisms for serious AI-related failures.

Concrete triggers for transitioning to Phase Three should include: (1) the operationalisation of at least one regulatory sandbox; (2) the publication of sector-specific AI guidelines by at least two sector regulators; and (3) demonstrated enforcement action by the Data Protection Authority in an AI-related matter.

Phase Three | Advancing mature AI governance frameworks

This phase focuses on enhanced oversight of high-risk AI systems (for example, automated administrative decision-making or credit assessments). Enhanced oversight mechanisms include periodic assessments, independent audits, technical documentation requirements, and ongoing monitoring, as well as comprehensive public-sector AI governance frameworks, national and regional registries for high-risk AI systems. This phase should also focus on enhanced support for local AI innovation ecosystems through research funding, local data initiatives, skills development programmes, computing infrastructure investments, and public-private collaboration, together with measures to promote affordable and equitable access to AI-enabled services across all communities, including through the achievement of minimum broadband penetration thresholds.

This phased approach set out above aligns with the AU AI Strategy's own implementation timeline, which envisions Phase 1 focusing on governance structures and Phase 2 on core project execution.¹⁰³ Governance frameworks should remain adaptive and technology-neutral. Given the pace at which AI capabilities are evolving, Vodacom recommends that governments favour principles-based guidance, periodic regulatory reviews, stakeholder consultation processes, and regulatory experimentation over highly prescriptive technical requirements.

Regional harmonisation and cross-border co-operation

AI systems, data flows, and the companies deploying them operate across national boundaries. **As countries develop national AI policies and regulatory frameworks, there is a growing risk that divergent approaches create unnecessary fragmentation.** Differing definitions, compliance obligations, reporting requirements, and oversight mechanisms increase regulatory complexity for businesses operating across multiple jurisdictions.

Fragmentation may also disproportionately affect African innovators and start-ups, who are less able than large multinational technology firms to absorb the costs of complying with multiple national regulatory regimes, thereby limiting their participation in the AI economy. Regional harmonisation can further the objectives of the AfCFTA and also contribute to more consistent protection of human rights across jurisdictions. Common principles, definitions and governance standards help reduce uncertainty regarding applicable protections and may strengthen confidence among citizens, businesses, and investors operating across borders.

The AU AI Strategy recognises these challenges and explicitly calls for increased continental cooperation, policy alignment, and collective engagement in global AI governance processes.¹⁰⁴ To this end, Vodacom recommends four concrete harmonisation mechanisms. First, African jurisdictions should adopt a shared risk-classification taxonomy for AI systems, aligned with the AU AI Strategy's risk-based principles, to ensure that the same AI application is governed consistently across borders. Without shared categories, a system classified as high-risk in one jurisdiction and low-risk in a neighbouring one creates regulatory arbitrage and undermines consumer protection.

Second, RECs should serve as the primary vehicles for regulatory harmonisation, developing model guidelines, and mutual recognition arrangements that REC member states can adopt. Given the slow pace of continental ratification processes, as evidenced by the Malabo Convention, REC-level coordination



Regional harmonisation and cross-border co-operation

continued

potentially offers a more realistic pathway than binding continental instruments.¹⁰⁵ Existing REC initiatives already align national policy approaches, promote common standards, facilitate cross-border data flows, and support interoperable digital infrastructure. Building on these mechanisms would promote regulatory coherence and regional market integration while advancing the practical conditions for cross-border AI development and deployment.

Third, national regulators should establish information-sharing protocols for AI-related incidents, enforcement actions, and regulatory innovations, drawing on existing cooperation mechanisms within the AU and RECs.

Fourth, the AU AI Strategy's proposed regional independent AI Ethics Board should be operationalised as a coordination and capacity-building platform, not a supranational regulator, to respect national sovereignty while enabling coherent governance across borders.¹⁰⁶

In line with its responsibilities under the AU AI Strategy, Vodacom's operational experience across multiple jurisdictions may usefully inform the design and testing of these harmonisation instruments.

CONCLUSION AND CONSOLIDATED RECOMMENDATIONS

Africa requires a principles-based, context-sensitive AI governance framework that enables responsible innovation, supports Africa's participation in the global AI economy, and expands equitable access to AI for all communities, while protecting human rights. Such a framework should draw on international best practice while adapting to the infrastructure constraints, institutional capacity limitations, and socio-economic realities that define the continent's regulatory environment. The uncritical adoption of any single international model is insufficient, while the constructive synthesis of transferable elements within an African-centred governance architecture is both feasible and urgent.

Accordingly, Vodacom respectfully puts forward the following consolidated recommendations to regulators and Ministers across its African operating jurisdictions:

- Adopt an AI governance framework grounded in human rights, fundamental freedoms and human dignity, and operationalised through the principles of transparency and explainability, accountability and human oversight, fairness and non-discrimination, safety and security, privacy and data protection, and proportionality;

- Establish a horizontal governance framework comprising common principles, terminology, risk-classification criteria, transparency obligations, accountability standards and rights-based safeguards, supplemented by sector-specific measures where necessary;
- Designate a lead AI coordination body with a defined legal mandate to set cross-sectoral AI standards, empower sector regulators to apply and enforce those standards within their domains, and utilise multi-stakeholder advisory mechanisms while building on existing institutional capacity;
- Implement phased compliance pathways aligned with institutional maturity, supported by documentation requirements, impact assessments, regulatory sandboxes and, where capacity permits, auditing, reporting and registry obligations;
- Invest in regulatory capacity, technical expertise, AI literacy, digital skills, data governance, digital infrastructure, cloud services, compute capacity and digital public infrastructure as foundational enablers of effective AI governance, and promote affordable and equitable access to connectivity, devices, and AI-enabled services so that all communities can benefit from, and participate in, the AI economy;
- Leverage RECs as the primary vehicles for regional harmonisation by aligning national AI policies, promoting common standards, facilitating trusted cross-border data flows, supporting interoperable infrastructure and advancing regional digital market integration; and
- Strengthen information-sharing and regulatory cooperation across African jurisdictions and engage private-sector actors as partners in implementation, capacity-building, infrastructure development and responsible innovation.

Taken together, these recommendations constitute a coherent and implementable governance architecture, grounded in international best practice, calibrated to African realities, and designed to evolve as institutional capacity matures and AI technologies advance.

Africa's AI governance moment is now. The frameworks established today will shape the continent's digital future for decades to come. The approach proposed here is intended to support regulators in building governance architectures that are principled, practical, and protective of the rights and aspirations of all Africans.

Endnotes

- ¹ Page 15 of “Continental Artificial Intelligence Strategy: Harnessing AI for Africa’s Development and Prosperity” published by the African Union in 2024, accessible here: https://au.int/sites/default/files/documents/44004-doc-EN-Continental_AI_Strategy_July_2024.pdf (the **AU AI Strategy**).
- ² Page 15 of “The Digital Transformation Strategy for Africa (2020 – 2030)” published by the African Union in 2020, accessible here: <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf> (the **AU DT Strategy**). See also “World Population Prospects 2024” published by the United Nations Department of Economic and Social Affairs, Population Division in 2024, accessible here: <https://population.un.org/wpp/>. The median age of the population in Sub-Saharan Africa is currently estimated to be 18.5 years old.
- ³ Page 2 of “The Mobile Economy Africa 2026” published by the GSMA in 2026, accessible here: https://www.itu.int/hub/publication/D-IND-ICT_MDD-2025-3/ (the **2026 GSMA Report**). In 2025, mobile technologies and services generated \$240-billion in economic value across Africa, supporting approximately 13-million jobs and contributing \$45-billion in public revenue.
- ⁴ Page 10 of “Measuring digital development: Facts and Figures 2025” published by the International Telecommunication Union in 2025, accessible here: https://www.itu.int/hub/publication/D-IND-ICT_MDD-2025-3/. As of 2025, at least 89% of the African population is covered by some type of mobile network. See also page 5 of the 2026 GSMA Report. Telecommunications network operators are expected to invest over \$76-billion in network infrastructure between 2024 and 2030, driving 5G penetration in Africa, which is expected to reach 21% in 2030.
- ⁵ Page 11 of “The State of the Industry Report on Mobile Money 2026” published by the GSMA in 2026, accessible here: <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2026/04/The-State-of-the-Industry-Report-2026-English.pdf>. Sub-Saharan Africa accounted for 66% of global mobile money transaction value in 2025, contributing \$1.4-trillion of the \$2.1-trillion total.
- ⁶ Page 4 of “The Mobile Economy of Sub-Saharan Africa 2024” published by the GSMA in 2024, accessible here: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf. See also page 2 of “Leading, not lagging: Africa’s gen AI opportunity” published by McKinsey in 2025, accessible here: [Gen AI in Africa: Unlocking potential | McKinsey](https://www.mckinsey.com/industries/technology-and-digital-transformation/our-insights/gen-ai-in-africa-unlocking-potential). McKinsey projects that “African economies could unlock up to \$100 billion in annual economic value across multiple sectors from gen AI alone” with “the combined traditional AI and gen AI total is more than double what gen AI can unlock on its own, with traditional AI making up at least 60 percent of the value.”
- ⁷ Pages 37 – 41 of the AU AI Strategy.
- ⁸ “Artificial Intelligence for Healthcare in Africa” published by Ayomide Owoyemi, Joshua Owoyemi, Adenekan Osiyemi and Andy Body in 2020, accessible here: <https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2020.00006/full>. See also section 3.3.4 of the AUDA-NEPAD AI Report.



Endnotes

continued

- ⁹ Page 4 of “*AI governance in Africa: Insights from a policy dialogue with 12 countries*” published by the Organisation for Economic Co-operation and Development (OECD) in 2026, accessible here: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/04/oecd-artificial-intelligence-case-studies_71322177/strengthening-ai-governance-in-africa_812bb149/1ff55135-en.pdf (the **OECD Dialogue Recap**). See also section 3.3.1 of the AUDA-NEPAD AI Report.
- ¹⁰ For instance, fraud and risk detection, credit scoring and assessments, and market surveillance. See “*Artificial Intelligence in the South African Financial Sector*” published by the South Africa Financial Sector Conduct Authority and the South African Prudential Authority in 2025, accessible here: <https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2025/artificial-intelligence-in-the-south-african-financial-sector/Artificial%20Intelligence%20in%20the%20South%20African%20Financial%20Sector.pdf> (the **FSCA Report**). See also section 3.3.7 of “*AI for Africa: Artificial Intelligence for Africa’s Socio-Economic Development*” published by AUDA-NEPAD in 2021, accessible here: <https://www.nepad.org/publication/ai-africa-artificial-intelligence-africas-socio-economic-development> (the **AUDA-NEPAD AI Report**).
- ¹¹ See, for instance, “*Artificial intelligence technologies usage for improved service delivery in Uganda*” published by Teddy Nalubega and Dominique E. Uwizeyimana in 2024, accessible here: <https://apsdpr.org/index.php/apsdpr/article/view/770/1612>. See also “*Governing with Artificial Intelligence: Are governments ready?*” published by the OECD in 2024, accessible here: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence_f0e316f5/26324bc2-en.pdf.
- ¹² Page 28 of the AU AI Strategy, which adopts a “*Local First*” guiding principle under which “*[t]he growth of local talent and ecosystems is considered paramount to advancing AI solutions that are of public value and interest, serving the Continent’s needs and priorities, and respecting and preserving cultural values and customs.*”; see also “*Conclusion*” of “*The State of AI in Africa – A Policy Brief*” published by the Centre for Intellectual Property and Information Technology Law at Strathmore University in 2025, accessible here: <https://cipit.strathmore.edu/wp-content/uploads/2026/02/the-state-of-ai-in-africa-report.pdf> (the **CIPIT Policy Brief**), which cautions that, absent investment in infrastructure, data ecosystems, talent, and contextualised, responsible AI regulations, African countries “*will continue to be consumers of tools and technologies developed without their consent, content, contribution and knowledge.*”
- ¹³ Pages 28 and 52 of the AU AI Strategy, which adopts an “*Inclusion and Diversity*” guiding principle under which “*[t]he production, development, use and assessment of AI in Africa will be inclusive, non-discriminatory, leaving no one and no place behind and benefiting everyone*”; see also page 65 of “*State of Internet Freedom in Africa 2025: Navigating the Implications of AI on Digital Democracy in Africa*” published by CIPESA in 2025, accessible here: <https://cipesa.org/2025/09/state-of-internet-freedom-in-africa-report/> (the **CIPESA Report**), which warns that unless infrastructure, connectivity, and skills gaps are addressed, AI will benefit connected urban populations while “*leaving out the poor, rural, marginalised and digitally excluded communities across the continent*”.
- ¹⁴ Pages 25 – 26 of the AU AI Strategy; pages 38 – 45 of the CIPESA Report; see also Chapter 1 of “*2025 Technology and Innovation Report*” published by the United Nations Conference on Trade and Development in 2025, accessible here: https://unctad.org/system/files/official-document/tir2025_en.pdf, which sets out some of the challenges posed by AI systems to developing countries generally.
- ¹⁵ Pages 26 – 27 of the AU AI Strategy, which provide that a “*lack of data is a barrier to developing solutions that use language understanding or speech recognition in different African languages*” and “*AI applications developed in other regions are likely to lack contextual relevance, particularly in terms of cultural and infrastructural factors, and will not be fit for purpose in Africa.*”
- ¹⁶ Page 65 of the CIPESA Report notes that, across Africa, “*digital infrastructure, connectivity, technical skills and literacy gaps remain the biggest bottleneck to AI adoption and usage*” and that regulatory institutions “*lack the necessary capacity, technical expertise, political independence and resources*” to enable proper oversight and accountability. In particular, page 15 of the AU DT Strategy notes that Africa’s low literacy rate undermines the achievement of proficient levels of digital literacy on the continent. This is supported in page 8 of “*The Tanzania National Artificial Intelligence Framework: Draft Version 6.0*” published by the Tanzanian Ministry of Communication and Information Technology in 2025, accessible here: [sw-1753973562-Final-Tanzania-NAI-Strategic-Framework-rev2-wTC - AN Commented - 31 July 2025 \(4\).pdf](https://www.mict.go.tz/wp-content/uploads/2025/07/sw-1753973562-Final-Tanzania-NAI-Strategic-Framework-rev2-wTC-AN-Commented-31-July-2025-4).pdf) (the **Tanzania AI Framework**), which provides that “*The public awareness and understanding of AI across communities remains low, particularly in rural and underserved areas. This lack of awareness can lead to resistance, mistrust, or misuse of AI systems and platforms. Digital literacy is vital for AI to be effectively integrated into society in Tanzania.*”; page 6 of “*The Economic Report: Data Centres in Africa*” published by the Africa Data Centres Association in 2026, accessible here: <https://africadca.org/wp-content/uploads/2026/03/DataCentresInAfrica2026-1.pdf?success=1789533283> (the **Africa Data Centres Association Report**), which notes that Africa accounts for less than 1% of global data centre capacity. See also page 45 of the “*Kenya Artificial Intelligence and Other Emerging Technologies Policy*” published by the Kenyan Ministry of Information, Communications and the Digital Economy in July 2026, accessible here: [draft-kenya-ai-and-emerging-technologies-policy-2026.pdf](https://www.micde.go.ke/wp-content/uploads/2026/07/draft-kenya-ai-and-emerging-technologies-policy-2026.pdf) (the **Kenya AI Policy**), which notes that only 5% of researchers on the continent have adequate compute access, citing “*Only five percent of Africa’s AI talent has the compute power it needs*” published by the United Nations Development Programme in 2024, accessible here: <https://www.undp.org/digital/blog/only-five-percent-africas-ai-talent-has-compute-power-it-needs>. See further page 3 of the OECD Dialogue Recap, which notes that: “*Weak data quality and governance constrain AI system reliability and trust. Inconsistent data standards, limited interoperability, incomplete data classification and uneven enforcement of data protection frameworks are among the key barriers.*”

Endnotes

continued

- ¹⁷ Page 6 of the OECD Dialogue Recap; “Responsible AI: Policies, Laws and Frameworks” of the CIPIT Policy Brief.
- ¹⁸ Pages 54 – 55, 57 – 58 of the AU AI Strategy.
- ¹⁹ Page 32 of the AU AI Strategy recommends that “African AI governance will consider emerging best practices both within the region and globally on AI policy and regulation”.
- ²⁰ Page 35 of the AU AI Strategy.
- ²¹ “Recommendation of the Council on Artificial Intelligence” adopted and published by the OECD Council in 2019, accessible here: <https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf> (the **OECD Recommendation**) establishes the OECD’s five “AI Principles”, namely (1) inclusive growth, sustainable development and wellbeing; (2) human-centred values and fairness; (3) transparency and explainability; (4) robustness, security and safety; and (5) accountability (the **OECD AI Principles**).
- ²² “The Recommendation on the Ethics of Artificial Intelligence” published by the United Nations Educational, Scientific and Cultural Organisation in 2021, accessible here: <https://unesdoc.unesco.org/ark:/48223/pf0000381137> (the **UNESCO Recommendation**).
- ²³ “G7 Hiroshima Process on Generative Artificial Intelligence: Towards a G7 Common Understanding on Generative AI” published by the OECD for the G7 Digital and Tech Working Group in 2023, accessible here: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/g7-hiroshima-process-on-generative-artificial-intelligence-ai_8d19e746/bf3c0c60-en.pdf (the **G7 Hiroshima Process**).
- ²⁴ “Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law” adopted in 2024, with reference number 225 in the Council of Europe Treaty Series, accessible here: <https://rm.coe.int/cets-225-en-docx/48802bf168> (the **European Framework Convention**).
- ²⁵ “Artificial Intelligence Risk Management Framework (AI RMF 1.0)” published by the US National Institute of Standards and Technology in 2023, accessible here: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.
- ²⁶ As noted in page 65 of “Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI” published by Jessica Fjeld, Nele Achyen, Hannah Hilligoss, Adam Christopher Nagy, and Madhulika Sri Kumar in 2020, accessible here: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482, most normative AI governance frameworks draw heavily on established principles of international human rights law. Common points of reference include the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the United Nations Guiding Principles on Business and Human Rights (**UNGPs**), and the United Nations Sustainable Development Goals. The UNGPs are particularly relevant in this context, having articulated the State duty to protect human rights and the corporate responsibility to respect human rights, while establishing human rights due diligence as a framework for identifying, preventing, mitigating, and accounting for adverse human rights impacts. The framework further contemplates human rights impact assessments, meaningful stakeholder engagement, the tracking of effectiveness of mitigation measures, and access to remediation where adverse impacts occur. These concepts have informed subsequent AI governance approaches concerned with addressing the human rights impacts associated with the development, deployment, and use of AI systems. See “Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework” (A/HRC/17/31) published in 2011, accessible here: <https://documents.un.org/doc/undoc/gen/g11/121/90/pdf/g1112190.pdf> (or in a more readable format here: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf), endorsed by the United Nations Human Rights Council in terms of Resolution 17/4 of 2011, accessible here: <https://docs.un.org/en/a/hrc/res/17/4>.
- ²⁷ Page 28 of the AU AI Strategy, which lists the following guiding principles: (1) local first; (2) people-centred; (3) human rights and human dignity; (4) peace and prosperity; (5) inclusion and diversity; (6) ethics and transparency; (7) cooperation and integration; and (8) skills development, public awareness and education.
- ²⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689 (the **EU AI Act**).
- ²⁹ Article 5 of the EU AI Act.
- ³⁰ Chapter III of the EU AI Act.
- ³¹ Article 50 of the EU AI Act.

Endnotes

continued

- ³² Article 99 of the EU AI Act.
- ³³ Sections 5.4.2 of “*Commission Staff Working Document Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence and amending certain Union legislative Acts*” published by the European Commission as COM(2021) 206 final, accessible here: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence> (the **EC Impact Assessment**).
- ³⁴ Section 6.1.3 of the EC Impact Assessment.
- ³⁵ Section 6.1.4 of the EC Impact Assessment.
- ³⁶ Sections 6.1.1 and 6.5 of the EC Impact Assessment.
- ³⁷ Paragraph 30 of “*A pro-innovation approach to AI regulation*” published by the UK Department for Science, Innovation & Technology in 2023, accessible here: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach> (the **UK White Paper**).
- ³⁸ Paragraph 48 of the UK White Paper. The principles are (1) safety, security and robustness; (2) appropriate transparency and explainability; (3) fairness; (4) accountability and governance; and (5) contestability and redress.
- ³⁹ Paragraphs 55 – 59 of the UK White Paper, which describes the “*period of non-statutory implementation*” during which the government will monitor the effectiveness of the non-statutory framework and, consequently, whether broader legislative changes will be required.
- ⁴⁰ Paragraph 34 of the UK White Paper.
- ⁴¹ “*Singapore National AI Strategy*” updated in 2026, accessible here: https://isomer-user-content.by.gov.sg/39/cb52d9a0-0d6c-484d-96fe-571031b37eb7/NAIS_update.pdf.
- ⁴² Including: “*Model Artificial Intelligence Governance Framework: Second Edition*” published by the Infocomm Media Development Authority (**IMDA**) and Personal Data Protection Commission in 2020, accessible here: [Model-AI-Governance-Framework-for-Generative-AI-19-June-2024.pdf](https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf); “*Model Governance Framework for Agentic AI*” published by the IMDA in 2026, accessible here: <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/mgf-for-agentic-ai.pdf>; “*Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem*” published by the IMDA in 2024, accessible here: <https://aiverifyfoundation.sg/wp-content/uploads/2024/06/Model-AI-Governance-Framework-for-Generative-AI-19-June-2024.pdf>; “*Starter Kit for Testing LLM-Based Applications for Safety and Reliability*” published by the IMDA in 2026, accessible here: [starter-kit-for-testing-llm-based-applications-for-safety-and-reliability.pdf](https://aiverifyfoundation.sg/wp-content/uploads/2024/06/Model-AI-Governance-Framework-for-Generative-AI-19-June-2024.pdf).
- ⁴³ “*AI Verify Testing Framework for Traditional and Generative AI*” published by the IMDA in 2023, accessible here: <https://file.go.gov.sg/aivtf-pdf.pdf>. The 11 AI governance principles on which the AI Verify Testing Framework is based are: (1) transparency; (2) explainability; (3) repeatability / reproducibility; (4) safety; (5) security; (6) robustness; (7) fairness; (8) data governance; (9) accountability; (10) human agency and oversight; and (11) inclusive growth, societal and environmental wellbeing.
- ⁴⁴ “*Navigating China’s regulatory approach to generative artificial intelligence and large language models*” by Mimi Zou and Lu Zhang published in the Cambridge Forum on AI: Law and Governance in 2025, accessible here: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/969B2055997BF42DE693B7A1A1B4E8BA/S033373324000048a.pdf/navigating-chinas-regulatory-approach-to-generative-artificial-intelligence-and-large-language-models.pdf>.
- ⁴⁵ “*Regulations on the Management of Algorithm Recommendations for Internet Information Services*” adopted in 2022, accessible here: https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.
- ⁴⁶ “*Regulations on the Management of Deep Synthesis in Internet Information Services*” adopted in 2022, accessible here: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm.
- ⁴⁷ “*Interim Measures for the Administration of Generative Artificial Intelligence Services*” adopted in 2023, accessible here: https://www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm, which establishes five principles for generative AI, namely: (1) upholding socialist core values; (2) taking effective measures to prevent discrimination; (3) respecting intellectual property rights and business ethics; (4) respecting others’ legitimate interests; and (5) taking effective measures to boost the transparency of generative AI services and the accuracy and reliability of content.
- ⁴⁸ Pages 32 – 33 of the AU AI Strategy.

Endnotes

continued

- ⁴⁹ Page 34 of the AU AI Strategy.
- ⁵⁰ Page 20 of the AU AI Strategy.
- ⁵¹ Page 50 of “*The SADC Digital Transformation Strategy and Action Plan*” (SADC/CM/2/2023/5.2.3B) adopted by the SADC in 2023, accessible here: https://www.sadc.int/sites/default/files/2025-08/EN - 5.2.3B - CM--SADC-ICT-INFO-MINISTERS-2023-4.8D - Draft SADC DTS_1.pdf (**SADC Digital Transformation Strategy**).
- ⁵² “*A Framework for Developing a National Artificial intelligence Strategy*” published by the World Economic Forum in 2019, accessible here: https://www3.weforum.org/docs/WEF_National_AI_Strategy.pdf.
- ⁵³ Page 46 of the SADC Digital Transformation Strategy.
- ⁵⁴ “*EAC Declaration on Artificial Intelligence*” adopted by the EAC in 2026, accessible here: <https://eabc-online.com/download/eac-declaration-on-artificial-intelligence/>.
- ⁵⁵ Page 40 of “*Seventh EAC Development Strategy 2026/27 – 2030/31: Comprehensive Planning and Implementation Matrix*” adopted by the EAC in 2026, accessible here: <https://www.eac.int/documents?controller=download&task=download.file&file=d0765521-f2db-4e14-9eed-5d4ac9dd52d5&name=7th%20EAC%20Development%20Strategy%20Implementation%20Matrix.pdf.pdf>.
- ⁵⁶ Page 2 of the OECD Dialogue Recap notes that translating the momentum in AI governance into effective outcomes “*requires addressing structural constraints that differ from those in higher-income economies, including infrastructure gaps, institutional capacity limitations and data governance challenges. These factors also shape which governance frameworks are feasible in practice. In this context, AI governance involves not only designing regulatory frameworks but also strengthening the technical, institutional, and human systems that enable their effective implementation*”.
- ⁵⁷ Page 46 of the Kenya AI Policy, citing pages 6 – 7 of “*The Economic Report: Data Centres in Africa*” published by the Africa Data Centres Association in 2026, accessible here: <https://africadca.org/wp-content/uploads/2026/03/DataCentresInAfrica2026-1.pdf?succes=1789533283>.
- ⁵⁸ Page 26 of the AU AI Strategy.
- ⁵⁹ Page 44 of the AU AI Strategy.
- ⁶⁰ Page 19 of “*Estratégia Nacional de Inteligência Artificial*” published by the Mozambican Ministry of Communications and Digital Transformation in July 2026, accessible here: https://bgonline-my.sharepoint.com/:b/g/personal/nerissa_naidoo_bowmanslaw_com/IQBASxSpwPz5TL95b1LI6nSEAVRiRnoiRdBJBIWJxfCUGrA?e=f2R3lx (the **Mozambique AI Strategy**), citing “*Digital 2026: Mozambique*” published by Datareportal in 2025, accessible here: <https://datareportal.com/reports/digital-2026-mozambique>.
- ⁶¹ Pages 9 – 10 of the Tanzania AI Framework.
- ⁶² Page 31 of “*Kenya AI Strategy 2025 – 2030: Implementation Roadmap*” published by the Ministry of Information, Communications and the Digital Economy in 2025, accessible here: https://ict.go.ke/sites/default/files/2025-12/Kenya_National_AI_Strategy_2025-2030_Implementation_Roadmap.pdf.
- ⁶³ Page 45 of the Kenya AI Policy.
- ⁶⁴ Page 12 of the Africa Data Centres Association Report; page 16 of the CIPESA Report.
- ⁶⁵ Page 65 of the CIPESA Report; page 33 of the Kenya AI Policy; and page 7 of the Mozambique AI Strategy.
- ⁶⁶ Accessible here: <https://au.int/sites/default/files/treaties/29560-treaty-0048 - african union convention on cyber security and personal data protection e.pdf>.
- ⁶⁷ “*List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection*” published by the African Union in 2026, accessible here: <https://au.int/sites/default/files/AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION %281%29.pdf>.
- ⁶⁸ “*List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection*” published by the African Union in 2026, accessible here: <https://au.int/sites/default/files/AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION %281%29.pdf>.

Endnotes

continued

- ⁶⁹ Page 45 of the Kenya AI Policy.
- ⁷⁰ “AU Data Policy Framework” published by the AU in 2024, accessible here: <https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf>. Page 5 of the AU Data Policy Framework, which lists the overarching objectives of the AU Data Policy Framework, including, among other things, to “ensure that data can flow across borders as freely as possible while achieving an equitable distribution of benefits and addressing risks related to human rights and national security” and “foster and facilitate cross border data flows and increase business opportunities while ensuring an adequate level of personal data and [sic] privacy”.
- ⁷¹ “Agreement Establishing the African Continental Free Trade Area” adopted by the African Union in 2018, accessible here: https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf. Article 3(a) of the AfCFTA provides that the objectives of the AfCFTA are to, among other things: “create a single market for goods, services” in order to “deepen the economic integration” of the continent.
- ⁷² A good example of this is the Mozambique AI Strategy, which (at page 68) emphasises the importance of identifying critical layers of the digital ecosystem where national control is necessary, while maintaining cooperation with international partners on balanced terms.
- ⁷³ Page 15 of the AU DT Strategy.
- ⁷⁴ Page 46 of the Kenya AI Policy.
- ⁷⁵ Page 8 of the Tanzania AI Framework.
- ⁷⁶ Page 16 of the AU DT Strategy.
- ⁷⁷ “Overview of the informal economy in Africa” published by the International Labour Organisation in 2025, accessible here: https://www.ilo.org/sites/default/files/2025-02/Africa_Informality%20Regional%20statistical%20profile.pdf.
- ⁷⁸ Page 25 of the AU AI Strategy; page 44 of the CIPESA report.
- ⁷⁹ See page 18 of the UNESCO Recommendation; page 4 of the AU AI Strategy.
- ⁸⁰ Paragraph 48 of the UK White Paper.
- ⁸¹ Page 18 of “Guide to Egypt National AI Governance Framework” published by the Egyptian National Council for Artificial Intelligence, Quantum Computing and Emerging Technologies in March 2026, accessible here: [https://ai.gov.eg/SynchedFiles/ar/Resources/Guide to Egypt%E2%80%99s National AI Governance Framework.pdf](https://ai.gov.eg/SynchedFiles/ar/Resources/Guide%20to%20Egypt%E2%80%99s%20National%20AI%20Governance%20Framework.pdf) (**Egypt Governance Framework**).
- ⁸² Pages 52 of “AI for Mauritius: A National Vision for Responsible AI and Regional Leadership” published by the Mauritian Ministry of Information Technology, Communication and Innovation on 13 February 2026, accessible here: <https://aim.govmu.org/aim/wp-content/uploads/2026/04/aistrategy.pdf> (**Mauritius AI Framework**).
- ⁸³ Pages 24 – 28 of the Kenya AI Policy.
- ⁸⁴ Pages 28 – 29 of “National Artificial Intelligence Strategy” published by the Nigerian Federal Ministry of Communication, Innovation and Digital Economy in September 2025, accessible here: <https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf>.
- ⁸⁵ Pages 25 – 26 of the Tanzania AI Framework.
- ⁸⁶ United Nations Human Rights Office of the High Commissioner, Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework (United Nations, 2011), available at: [Guiding Principles on Business and Human Rights](https://www.unhcr.org/refugees/4d4b4d4d.html).
- ⁸⁷ See, for instance, articles 14 (Human oversight) and 86 (Right to explanation of individual decision-making) of the EU AI Act; and paragraph 50 of the UK White Paper. See also pages 32 – 35 of “Human Rights in the Age of Artificial Intelligence” published by Access Now in 2018, accessible here: <https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf>, which recommends specific interventions for both state and non-state use of AI; and page 59 of the CIPESA Report.

Endnotes

continued

- ⁸⁸ Page 53 of the AU AI Strategy.
- ⁸⁹ Page 65 of “*Global Trends in AI Governance: Evolving Country Approaches*” published by the World Bank Group in 2024, accessible here: [Open Knowledge Repository](#) (the **World Bank Report**).
- ⁹⁰ African jurisdictions that have adopted the EU’s risk based model, but calibrated it to local conditions include Egypt: page 6 of the Egypt Governance Framework sets out Egypt’s risk-based approach, which classifies AI systems into four risk tiers, namely (1) prohibited (i.e., systems posing unacceptable risks to sovereignty or fundamental rights); (2) high risk (i.e., critical infrastructure and biometrics); (3) limited risk (i.e., chatbots and deepfakes); and (4) minimal risk (i.e., standard software tools); and Mauritius: page 12 – 16 of the “*FAIR Guidelines for the Development and Use of Artificial Intelligence*” published by the Ministry of Information Technology, Communication and Innovation on 9 April 2026, accessible here: <https://aim.govmu.org/aim/fair-guidelines/> (**Mauritius FAIR Guidelines**), which establish four risk tiers, namely (1) low-risk systems (i.e., applications with limited impact, typically used to support routing tasks or everyday activities where errors are unlikely to cause harm or serious consequences); (2) medium-risk systems (i.e., applications that influence decisions or processes in ways that have noticeable effects on people, but where human judgement remains involved and outcomes can usually be reviewed, adjusted or corrected); (3) high-risk systems (i.e., applications used in sensitive or important contexts where errors, bias or misuse could lead to significant harm, unfair treatment, loss of rights, exclusion from essential services or serious loss of public trust); and (4) unacceptable risk (i.e., uses of AI which raise fundamental concerns because of their potential impact on human dignity, fundamental rights, or the public interest).
- ⁹¹ With the exception of Kenya and Mozambique, which currently set out the estimated resources required to establish the proposed regulatory bodies and to conduct their work. See Annex 1 of the Kenya AI Policy and page 70 of the Mozambique AI Strategy.
- ⁹² “*Rethinking Africa’s Approach to the Politics of AI Governance and Regulation*” published by CIPESA in 2026, accessible here: <https://cipesa.org/2026/07/rethinking-africas-approach-to-the-politics-of-ai-governance-and-regulation/>.
- ⁹³ This approach has been adopted in Mauritius, which empowers sector regulators to issue context-specific guidelines under the FAIR framework (pages 50 and 53 of the Mauritius AI Framework, page 16 of the Mauritius FAIR Guidelines); Kenya, which proposes a National AI and Emerging Technologies Council with coordinating authority (pages 78 – 83 of the Kenya AI Policy); and Egypt, which centres the National Council for AI as the strategic architect while distributing operational functions to its technical arm, the Egyptian Centre for Responsible AI, and sectoral regulators (pages 13 – 17 of the Egypt Governance Framework).
- ⁹⁴ Pages 73 – 77 of the World Bank Report, which undertakes a comparative analysis of different institutional models. See also page 51 of the CIPESA Report, which describes the institutional weaknesses of overlapping responsibilities among institutions and a lack of dedicated, empowered AI governance bodies.
- ⁹⁵ Policy Area 1 of the UNESCO Recommendation.
- ⁹⁶ Page 33 of the AU AI Strategy.
- ⁹⁷ Page 33 of the AU AI Strategy.
- ⁹⁸ Page 55 of the Kenya AI Policy.
- ⁹⁹ Page 38 of the Mozambique AI Strategy.
- ¹⁰⁰ Page 30 of the Egypt Governance Framework.
- ¹⁰¹ See, for instance, Annexure III of the EU AI Act; page 64 of the Kenya AI Policy; and page 29 of the Mauritius FAIR Guidelines.
- ¹⁰² Page 32 of the AU AI Strategy, which provides that “*amendment and application of existing laws and frameworks*” is a “*crucial first step*”, followed by the “*identification of regulatory gaps*” in response to which the flexible and adaptable AI regulation legislation models should be applied. This approach has been adopted in Kenya, Tanzania, Nigeria, and Ghana.

Endnotes

continued

- ¹⁰³ Pages 60 – 61 of the AU AI Strategy.
- ¹⁰⁴ Pages 56 – 57 of the AU AI Strategy.
- ¹⁰⁵ Pages 7, 28, 55, 57, 59 – 60 of the AU AI Strategy recognise the key role of RECs in AI governance on the continent.
- ¹⁰⁶ Page 35 of the AU AI Strategy.



Further together