TECH HIVE ADVISORY

December 2025

THE YEAR OF THE TEETH:

Data Protection Roundup in Africa, 2025, and Projections for 2026

Digital Policy Alert

PRIVACY GUIDE AFRICA

PRIVACY LENS AFRICA

Ulinzi

About Tech Hive™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm providing services to private and public organisations regarding the intersection between technology, business, and law. While acting as an innovation partner for our clients, we focus on how emerging and disruptive technologies are changing and influencing traditional ways of doing things. We focus on how emerging and disruptive technologies are altering and influencing traditional ways of doing things while acting as an innovation partner to our clients.

Our expertise and experience span Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Regulatory Intelligence, Start-Up Advisory, Emerging Tech, and Digital Health. We ensure that our advice is useful to our clients by thoroughly understanding their businesses and the markets in which they operate, which we accomplish through accurate policy and legislative development tracking and intelligence.

contact@techhiveadvisory.africa

About Digital Policy Alert

The **Digital Policy Alert (DPA)** is a Swiss non-profit devoted to transparency in digital policy. The Digital Policy Alert is a public and independent repository of policy changes affecting the digital economy. Established in 2021, DPA has documented thousands of policy changes covering more than a dozen policy areas from 50+ jurisdictions. DPA consistently monitors government policies and regulatory developments that impact the digital economy. Based on robust policy datasets, DPA provides expert oversight of regulations and topical threads, curates digital digests, and develops comprehensive regulatory reports. If you have feedback or questions on DPA, please contact Maria Buza.

info@digitalpolicyalert.org.

About Privacy Guide Africa

Privacy Guide Africa (PGA) is a free online tool that helps organisations across the African continent understand and meet their data protection and privacy obligations under local laws, making what can be a confusing process much simpler and clearer. It offers practical assessment modules and resources so businesses and institutions can check their compliance with national data protection requirements and improve their privacy practices.

www.privacyguide.africa

About Privacy Lens Africa

Privacy Lens Africa (PLA) is your go to source for understanding data protection laws and trends across the African continent. The PLA's Africa Data Protection Series aims to provide a snapshot of Africa's data protection landscape by delving into the nuances that distinguish Africa's data protection laws. This series will demonstrate how these laws differ and overlap through blogs and interactive infographics. This descriptive analysis will serve as a foundation for any future analysis of the state of data protection in Africa.

Africa is a continent that is rapidly embracing technology, and with this comes the need for adequate protection of personal data. Privacy Lens Africa is dedicated to educating individuals, businesses, and organisations on the state of data protection laws in Africa.

hello@privacylens.africa

About Ulinzi

Ulinzi is a privacy compliance software solution with a mission to empower African businesses to achieve effortless privacy compliance. Dataulinzi provides the knowledge and tools needed to navigate the complex and evolving regulatory landscape, reduce risk, and build trust with data protection stakeholders across the continent through automation.

hello@dataulinzi.com

Authors

Ridwan Oloyede
Victoria Adaramola
Maria Buza

Contributors

Precious Nwadike, Olamiposi Aluko, Lauretta Onwuegbuzie, Wisdom Agbonyehemen, Feranmi Ekundayo, Samuel Akinrinola, Deji Sarumi, Dorcas Tsebee

Design and layout: Rachael Olujimi

Disclaimer - Usage of Publication

The report is intended to be general and educational in nature and should not be construed as legal advice. The report's findings and materials may not apply to all circumstances. Therefore, they should not be acted upon without obtaining specific legal counsel based on the circumstances. The absence of a trademark or service mark from this list does not imply that Tech Hive has waived its intellectual property rights regarding that name, mark, or logo.

Acknowledgement

We appreciate our esteemed speakers, Danielle Moukouri, Dorine Wanjeru, Gaspar Micolo and our moderators, Rachel Magege and Victoria Adaramola, for their invaluable contributions during our Hive Pulse Point (Roundup Edition) event titled *"**The State of Data Protection and AI Regulation in Africa:** 2025 at a Glance and Projections for 2026."* The speakers shared insights on the data protection and AI governance landscapes in Africa, which informed some of our projections in this report.

List of Abbreviations

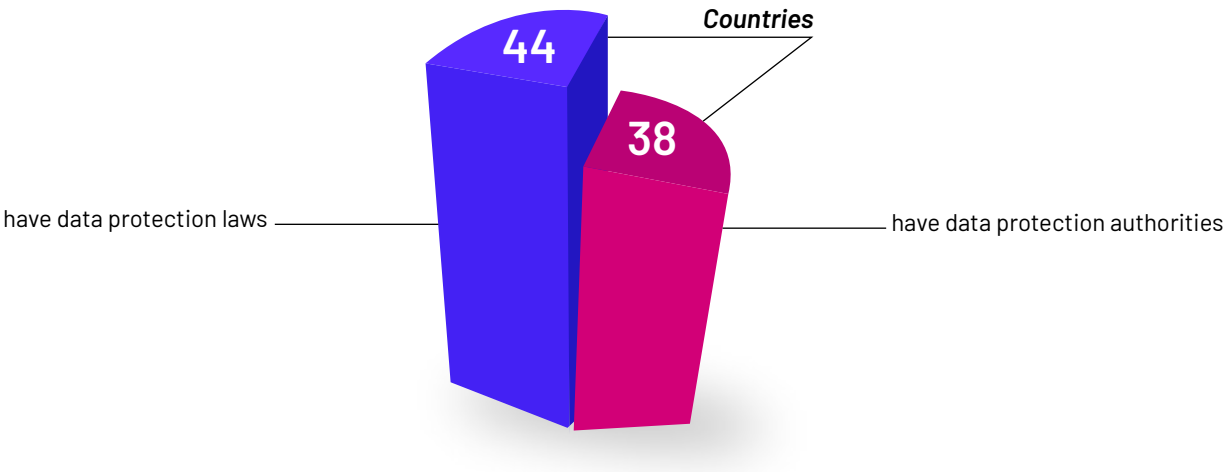
AFAPDP	Association of Francophone Data Protection Authorities
AfCFTA	African Continental Free Trade Agreement
AI	Artificial Intelligence
APD	Agencia de Proteção de Dados
APDP	Personal Data Protection Authority
APDPVP	Authority for the Protection of Personal Data and Privacy
ARTCI	Autorite De Regulation Des Telecommunications De Cote D'Ivoire
AU	African Union
APET	African Union High-Level Panel on Emerging Technologies
AUDA-NEPAD	African Union Development Agency
BCRs	Binding Corporate Rules
CBPR	Cross Border Privacy Rules
CDP	Commission des Données Personnelles
CNDP	Commission Nationale pour la Protection des Données
COS	Child Online Safety
DGIFA	Data Governance and Innovation Forum for Africa
DPA	Data Protection Authority
DPF	African Union's Data Policy Framework
DPO	Data Protection Officer
DMASA	Direct Marketing Association of Southern Africa
DRC	Democratic Republic of Congo
FPB	Films and Publications Board
ECOWAS	Economic Community of West African States
EDPA	Eswatini Data Protection Authority
ESCCOM	Eswatini Communications Commission
EU	European Union
GPA	Global Privacy Assembly
HAPDP	High Authority for Personal Data Protection
ICT	Information and Communication Technologies
IPU	Inter-Parliamentary Union
INPDP	Instance Nationale de Protection des Données Personnelles
ITU	International Telecommunication Union
KMPDC	Kenya Medical Practitioners and Dentists Council

MACRA	Malawi Communications Regulatory Authority
MOU	Memorandum of Understanding
NADPA	Network of African Data Protection Authorities
NCC	Nigerian Communications Commission
NCSA	National Cyber Security Authority
NDPC	Nigeria Data Protection Commission
NDPR	Nigeria Data Protection Regulation
NDPA	Nigeria Data Protection Act
NDP Act GAID	Nigeria Data Protection Act, General Application and Implementation Directive
NITDA	National Information Technology Development Agency
ODPC	Office of the Data Protection Commissioner
PDPL	Personal Data Protection Law
PDPO	Personal Data Protection Office
POPIA	Protection of Personal Information Act
SADC	Southern African Development Community
SCCs	Standard Contract Clauses
SOP4COP	Standard Operating Procedures for Child Online Protection in Nigeria
UCC	Uganda Communication Commission
UNICEF	United Nations International Children's Emergency Fund
EARFAI	UNESCO-Eastern Africa Sub-Regional Forum on Artificial Intelligence

Executive Summary

If the last decade of data protection in Africa was defined by the adoption of laws, 2025 will be remembered as the year those laws grew teeth. This report chronicles a decisive shift in the regulatory landscape. The region has transitioned from an era of theoretical compliance to one of tangible enforcement. Regulatory bodies have evolved from passive observers to active enforcers—adjudicating disputes, levying fines, and securing convictions.

The continent has reached critical mass. With 44 countries now having data protection laws—representing 80% of African Union member states—and 38 fully operational Data Protection Authorities, the oversight infrastructure is largely in place. In 2025, this infrastructure was operationalised. Regulators across the continent moved beyond awareness campaigns to aggressive enforcement. The "grace period" is officially over.



This maturity manifested in three distinct ways during the year:

1. Authorities are issuing significant financial penalties for non-compliance. More critically, regulators are piercing the corporate veil; criminal convictions in Uganda and prison sentences in South Africa for data offences signal that executives now face personal liability for privacy failures.

2. The courts have emerged as the true arbiters of digital norms. From halting biometric data collection in Kenya to awarding damages for SIM swaps in Egypt and intrusive robocalls in Nigeria, the judiciary is establishing that corporate negligence carries a tangible price tag.

3. Traditional regulatory silos are being dismantled. Competition authorities and consumer protection bodies are increasingly asserting jurisdiction over data governance. The "Gatekeeper" approach adopted by COMESA and South Africa treats data accumulation as a metric of market dominance, blending antitrust law with privacy concerns.

While enforcement on traditional data issues tightened, governance strategies for emerging technologies hardened. The discourse on Artificial Intelligence has decisively shifted from high-level ethical consensus to binding statutory mandates. Nigeria, Angola, and Morocco are racing to enact the continent's first dedicated AI legislation, moving away from voluntary guidelines to strict statutory compliance.

Simultaneously, digital sovereignty took centre stage. Nations are increasingly demanding that global platforms play by local rules. Measures ranging from data localisation requirements in Kenya and Ghana to the "digital sovereignty" bills in Algeria and Nigeria demonstrate a collective intent to end the era of digital extraterritoriality.

Projections for 2026: The Year of Agility

Looking ahead, 2026 will likely see Africa surpass 50 data protection laws. We project the enactment of the continent's first comprehensive AI laws by the second quarter, alongside a surge in sector-specific regulations for high-risk industries like finance and health. The regulatory environment will become more experimental yet more severe. We anticipate the launch of regulatory sandboxes to prototype policies in real time, alongside a rise in criminal prosecutions for egregious violations. Furthermore, the map of international data flows will be redrawn as countries such as Kenya push for EU adequacy and others pivot toward the Global Data Privacy Rules system.

Conclusion

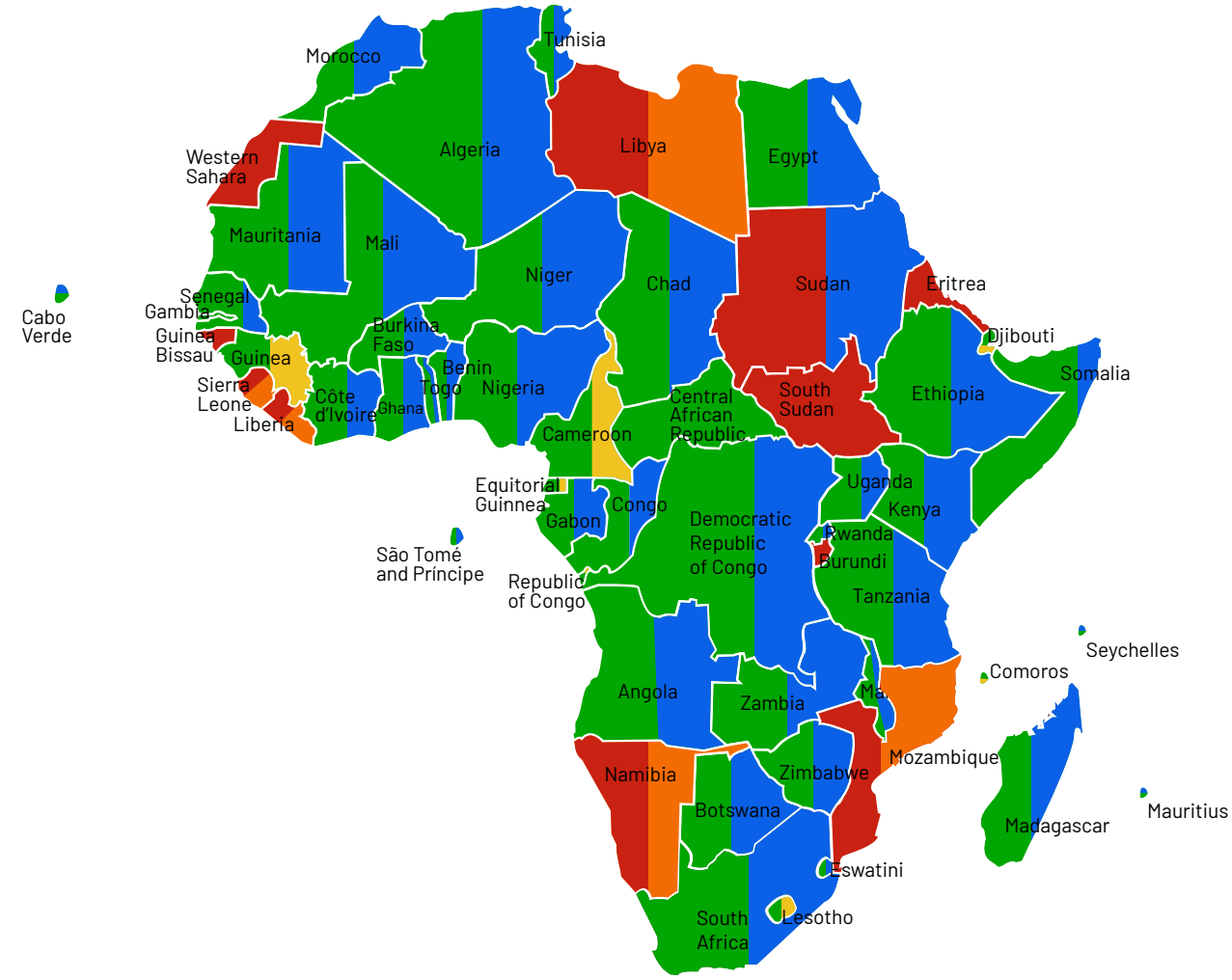
The "Year of the Teeth" proved that African data protection is no longer a theoretical exercise. The ecosystem is evolving into a muscular, complex regulatory environment where cross-border collaboration is the norm and "lack of awareness" is no longer a valid defence. For organisations operating in Africa, the 2026 strategy cannot be limited to static compliance; it must embrace strategic agility. As regulators sharpen their tools and courts define the red lines, the only path forward is proactive, ethical engagement that anticipates, rather than reacts to, the biting reality of the law.

Introduction

If the last decade of data protection in Africa was defined by the adoption of laws, 2025 will be remembered as the year of consequences. Calling it the "Year of the Teeth" does not overstate the progress made; it highlights the ecosystem's rising maturity. It was a year defined by heightened judicial scrutiny, enforcement, larger fines, and—critically—criminal convictions.

The era of the "paper tiger" is fading. Regulators are no longer just existing; they are adjudicating. We moved from an era of theoretical compliance to one of tangible enforcement and complex convergence. The silos separating data protection, competition law, and consumer protection are blurring, creating a new, multidimensional regulatory environment in which a violation is no longer just a compliance failure—it is a market issue and a potential criminal liability.

This report synthesises developments over the last 12 months, drawing on legislative activity, enforcement actions, and strategic policy shifts across the continent. It also looks forward, offering concrete projections for 2026—a year we anticipate will see Africa cross the threshold of 50 data protection laws and 40 operational authorities.



Countries with draft laws:

Liberia, Sierra Leone, Namibia, Mozambique and Libya.

- Countries with laws (44)
- Countries with laws and authorities (38)
- Countries with laws without authorities (6)
- Countries without data protection laws (11)

Part I: The 2025 Retrospective

1. The Legislative "New and Second Wave"

While early adopters focused on enforcement, a "new and second wave" of legislation emerged to fix gaps in initial laws and bring holdout countries into the fold. Djibouti adopted its Digital Code in June, which incorporated its data protection law. The Gambia enacted its law, and similarly, Botswana's amended Data Protection Act of 2024 came into effect in January. Beyond new laws, the existing laws are evolving. Algeria completed amendments to its data protection law, introducing new obligations regarding DPO appointments and stricter breach notification timelines.

	Country	Law
	Algeria	Amendment to the Data Protection Law
	Botswana	Data Protection Act
	Djibouti	Digital Code. The Digital Code contains the Data Protection Law.
	The Gambia	Personal Data Protection and Privacy Act

Ghana is in the process of amending several data protection frameworks. The amendments to the Data Protection Act 2012 would introduce rules on the processing of children's and sensitive data, establish data retention limits and international data transfer rules, and require data protection impact assessments and privacy by design. Amendments to the Electronic Communications Act 2025 and the draft Cybersecurity (Amendment) Bill would extend data protection obligations to electronic communications and broadcasting service providers, set conditions for metadata retention, and regulate government access to data. Similar amendment processes are currently underway in Angola, Kenya, Mauritius, Nigeria, and Senegal, reflecting a desire to close legislative loopholes. While Liberia, Mozambique, Namibia, and Sierra Leone have made progress on their draft laws, South Sudan has indicated it plans to introduce a law in 2026.

2. Institutional Maturity: The New Custodians

The continent's regulatory map has been filled in substantially this year. Currently, at least 44 countries have enacted data protection laws, representing 80% of African Union member states—a figure set to rise as pending bills proceed in the coming year. Of these, at least 38 countries have fully established Data Protection Authorities (DPAs), leaving only six with laws but no operational regulator, and 11 countries yet to legislate.

The "paper law" era ended for more countries this year, as they inaugurated enforcement bodies and adopted varied structural models. The Republic of Congo and Togo established their respective standalone authorities, which were operationalised in March. Others took a pragmatic approach by empowering existing regulators: Malawi designated the Malawi Communications Regulatory Authority as the DPA in January, and the Gambia designated its Information Commission. In a rare procedural twist, Sudan established the Sudanese Data and Artificial Intelligence Authority, effectively creating an institution to oversee data governance even before enacting a primary data protection law. This institutional growth culminated in the admission of Somalia and Tanzania as members of the Network of African Data Protection Authorities (NADPA), signalling a robust expansion of the pan-African regulatory network.

	Country	Authority
	The Gambia	Information Commission
	Malawi	Malawi Communications Regulatory Authority
	Sudan	Sudanese Data and Artificial Intelligence Authority
	Republic of Congo	National Commission for the Protection of Personal Data

3. The Operationalisation of Law: From Ambiguity to Clarity

With institutions in place, authorities shifted their focus from mere existence to active hand-holding, bridging the gap between high-level law and daily operations. Nigeria led the charge with the General Application and Implementation Directive in March, which took effect in September. South Africa's Information Regulator published amendments to the Regulations Relating to the Protection of Personal Information that significantly clarified the rights to object, erasure, and rectification, and introduced a strict 30-day processing timeline. The amendments also mandated documented consent for direct marketing and introduced instalment payment plans for administrative fines.

Kenya followed suit with a comprehensive suite of eight guidance notes covering critical areas: Children's Data, Biometric Data, Recorded Media, Research, Journalism, MSMEs, the Public Sector, and Historical/Statistical Purposes. Additionally, Kenya ODPC published the draft Data Sharing Code to establish frameworks for lawful data sharing between entities, and the Data Protection (Conduct of Compliance Audit) Regulations, to establish procedures for assessing organisational compliance with data protection obligations. Algeria released a compliance package for processing personal data to support the implementation of the Data Protection Law. It includes guidelines on compliance procedures and four templates covering confidentiality agreements, consent notices, IT security charters, and subcontractor agreements. Zambia also published the terms and conditions and the guidelines for registration as a data controller and processor. Zimbabwe published a licensing guideline laying out detailed requirements for data controllers under its law. Similarly, Malawi operationalised its new mandate by publishing regulations on Personal Data Breach Notifications, Compliance Guidelines, Data Processor Engagement, and Complaints and Investigations. Egypt published its long-awaited executive regulation, which has now fully operationalised the 2020 data protection law. Consequently, the Personal Data Protection Centre (PDPC) will now enforce the law. The executive regulation requires data controllers and processors that process personal data to obtain specific regulatory licenses for processing and cross-border transfers, register certified Data Protection Officers with the PDPC, and strictly adhere to a 72-hour window for reporting data breaches.This flurry of activity signifies that regulators are prioritising operational clarity, acknowledging that sustainable compliance requires practical, distinct roadmaps rather than generic legal threats.

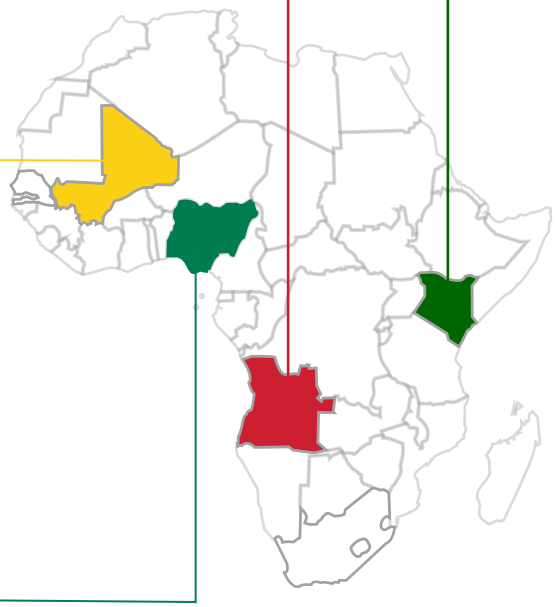
4. Enforcement: The "Year of the Teeth."

Country	**Angola**
Authority	Data Protection Authority
Institution	An Airline
Sanction /Decision	175,000 USD
Violation	Failing to implement appropriate technical safeguards and obtain authorisation before processing personal data

Country	Mali
Authority	Personal Data Protection Authority
Institution	Koulakou Medical Clinic
Sanction /Decision	5,000,000 CFA
Violation	Refusing to allow the Authority to conduct an inspection

Country	**Nigeria**
Authority	Nigeria Data Protection Commission
Institution	Multichoice
Sanction /Decision	₦766,242,500 (approximately USD 500,481)
Violation	Investigations concluded that the company's processing activities violated Nigerians' privacy and involved illegal cross-border transfers of Nigerian data.

Country	**Kenya**
Authority	Office of the Data Protection Commissioner
Institution	Hotel Tobriana
Sanction /Decision	750,000 KES
Violation	Using a data subject and their relative's data for commercial purposes without obtaining consent



TECH HIVE ADVISORY

With the rules clarified, regulators moved to policing. There was a significant increase in both enforcement appetite and the scale of actions. For instance, as of this writing, Kenya's Office of the Data Protection Commissioner (ODPC) has published over 110 decisions this year alone, underscoring its operational intensity. Notably, the ODPC fined a digital lending company KES 700,000 (approximately USD 5,400) for unlawfully processing personal data by wrongly associating a data subject with a loan they had not taken and for failing to cooperate with the investigation. The ODPC also fined a company 750,000 KES (approximately 5,791 USD) for using the images of a data subject and his relative for commercial purposes without obtaining consent. In Nigeria, the Nigeria Data Protection Commission (NDPC) continued to pressure major entities, fining a leading digital satellite television provider ₦766 million (approximately USD 500,481) for privacy breaches and illegal cross-border transfers. A high-profile dispute with a major international social media platform, which began when the NDPC imposed a $32.8 million fine in February for alleged data violations, was resolved in November through an out-of-court settlement.

In South Africa, the Information Regulator reached a settlement with a major instant messaging service. This agreement mandates enhanced user transparency and resolves an enforcement notice issued under the Protection of Personal Information Act. Enforcement activity was equally robust in Mali, where the Personal Data Protection Authority (APDP) fined a company 5,000,000 CFA (approximately USD 8,766) for refusing to allow an inspection. The APDP also issued an enforcement notice against the same company for failing to report its processing activities, emphasising that obstructing its agents constitutes an offence punishable by up to 20,000,000 CFA (approximately USD 35,242). Similarly, in Angola, the Data Protection Authority imposed a USD 175,000 fine on an airline for failing to implement appropriate technical safeguards and obtain authorisation before processing personal data. The Eswatini Data Protection Authority issued a formal warning and strict directives to an organisation after finding it had failed to secure sensitive data or notify the regulator of a resulting breach. This enforcement action required an apology within 48 hours and a comprehensive Data Protection Impact Assessment (DPIA) for the entity's human resources department, signalling a move toward rigorous operational accountability.

Regulators have also adopted a "deadline-driven" approach, indicating a drift from awareness to enforcement. The Ghana Data Protection Commission issued a stern ultimatum to data controllers, warning that it would commence a rigorous prosecution drive in January against non-compliant entities, and also unveiled a privacy seal as evidence of trust and compliance, empowering citizens to instantly verify an organisation's compliance status, effectively deputising the public to monitor accountability. This follows a year of amnesty and awareness, signalling that the "grace period" for registration and compliance has officially expired. The Commission also announced that it is investigating a data breach involving a healthcare solution, with unauthorised access to patient data. Morocco's CNDP announced it would issue formal warnings to companies in high-risk sectors—specifically healthcare, legal services, and media. The CNDP warned that failure to regularise their status would result in immediate penalties, emphasising that the sensitivity of data in these industries permits no room for negligence. Kenya's ODPC issued a similar warning to the hospitality industry. Also, the Commission launched a major enforcement drive in August 2025 to assess adherence to data processing principles, implementation of privacy-by-design requirements, and fulfilment of data subject rights obligations, issuing compliance notices to more than 1,300

organisations across key economic sectors. In South Africa, the Information Regulator launched a deep investigation into the caller identification app following a flood of complaints from businesses and individuals in mid-2025. Similarly, Burkina Faso's Commission for Information Technology and Liberties significantly strengthened its enforcement toolkit by approving a new administrative sanction framework that empowers it to escalate from simple compliance notices to imposing financial penalties and public disclosure. The new procedure sets clear timelines of up to three months for resolving complaints and investigations, signalling that the era of leniency is ending. These warnings indicate that regulators are no longer accepting "lack of awareness" as a valid defence, particularly in industries that handle high volumes of sensitive personal data.

2025 also proved that borders are no longer barriers to enforcement. In a precedent-setting move, Kenya's ODPC and Uganda's PDPO conducted a joint investigation into a commercial bank following a system integration failure that exposed customer data across both jurisdictions. The collaboration led to sanctions, which rejected the "human error" defence and emphasised that system failures are ultimately governance failures. This coordinated action signals to multinational entities that they can no longer play "regulatory arbitrage" between African countries.

a. Litigation: Courts Defining the Red Lines

While regulators levied fines, the judiciary emerged as the true arbiter of data protection norms, establishing that corporate negligence now carries a tangible price tag. In Egypt, the Alexandria Economic Court issued a landmark ruling against a major telecom, fining the company EGP 10 million (approximately USD 200,853) for an unauthorised SIM swap. The court established that telecommunications providers are "custodians" of data with an affirmative duty to prevent fraud, applying data protection principles even before the law's full operationalisation. Kenya saw the courts intervene early in the deployment of facial recognition (biometric technology). In a case involving the Kenya Broadcasting Corporation, the court declared the use of facial biometric clock-in systems for workers illegal and ordered the deletion of the collected data. This judgment sets a critical precedent for employee privacy, signalling that "efficiency" is not a blanket justification for intrusive workplace data collection. Similarly, a Kenyan High Court halted the operations of a global biometric identity platform, ruling that the mass collection of iris scans violated the constitution for failing to conduct a proper Data Protection Impact Assessment. This judgment reinforced that DPIAs are not merely bureaucratic checkboxes but mandatory prerequisites for high-risk processing activities.

In Nigeria, the courts defended the rights of data subjects against financial institutions. A High Court awarded ₦5 million (approximately USD 3,400) in damages to a customer against a commercial bank for altering and deleting transaction records, resulting in the customer losing a property deal valued at ₦200 million. In a separate judgment, the Federal High Court awarded damages against a microfinance bank for intrusive robocalls, issued a perpetual injunction against the company, and ordered a formal apology. These decisions confirm that Nigerian courts are willing to award general damages for data rights violations, dismissing standard defences of negligence or contractual oversight.

Tanzania reinforced the sanctity of consent in commercial contracts. The High Court awarded 40 million TZS (approximately USD 14,866) to the subject against two companies that continued to use the subject's image in marketing after the contract had expired. Uganda expanded the boundaries of privacy to the deceased. The High Court dismissed a request to access a deceased person's will, ruling that privacy rights persist post-mortem. Collectively, these rulings demonstrate that the judiciary is emerging as a decisive force in data governance, bridging the gap between legislative intent and practical enforcement. Beyond imposing fines, the courts also issued crucial clarifications on the procedures for seeking redress for violations of data protection laws in Kenya and Nigeria. In Kenya, the court affirmed the ODPC's powers to address privacy violations in the first instance before the matter is brought before the court. The Nigerian High Court made a contrasting decision, stating that lodging a complaint with the NDPC before approaching the court is discretionary and that data subjects could approach the courts directly. These judicial interventions across the continent underscore a growing trend toward heightened enforcement, in which courts are actively defining the scope and practical application of the law.

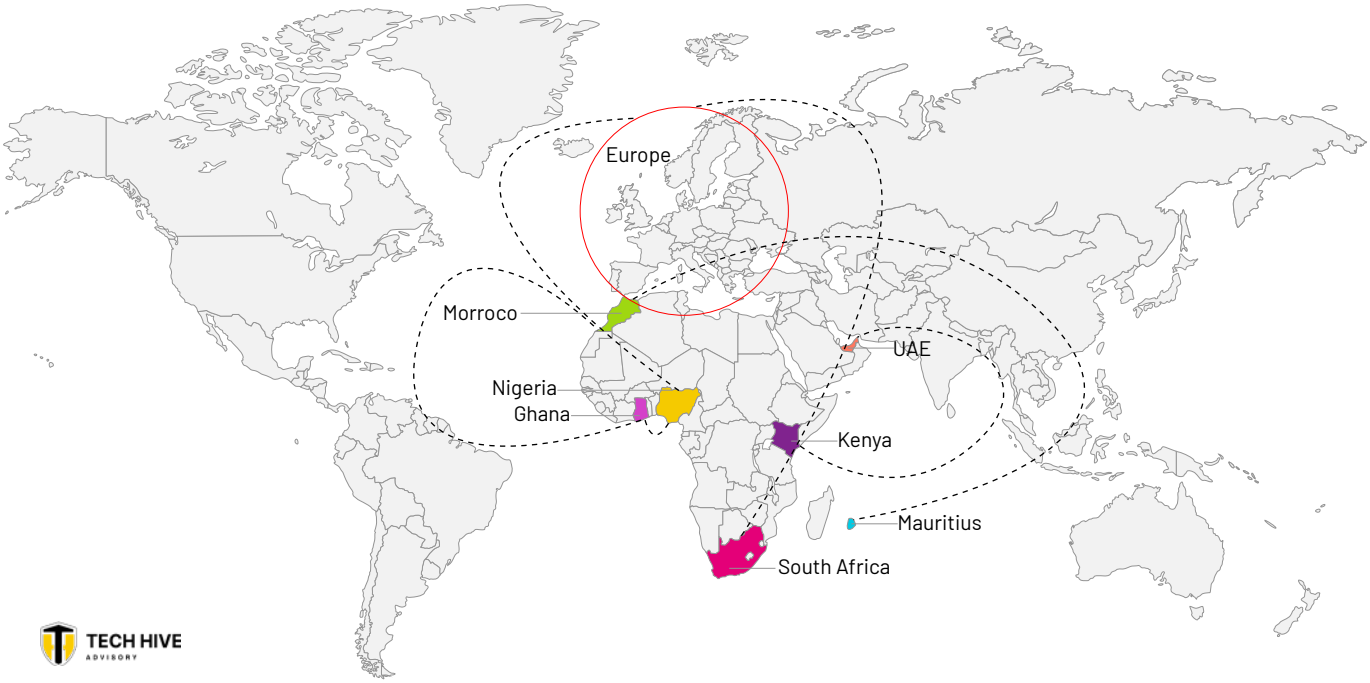
b. Criminal Liability

2025 also shattered the assumption that data protection violations are merely administrative nuisances. Uganda recorded two criminal convictions for data protection offences this year, signalling a robust shift toward criminal enforcement. Similarly, a South African court sentenced a company employee to eight years' imprisonment for installing software that facilitated a ransomware attack. This severe sentence highlights the growing intolerance for insider threats and the criminalisation of actions that compromise data security.

5. International Data Transfers

As cross-border data flows became critical for digital trade, African countries intensified their efforts to secure their status as trusted data hubs. Mauritius and Morocco led on one front, disclosing an intention to renegotiate to secure an EU adequacy decision and positioning themselves as prime destinations for outsourcing. Kenya continues its dialogue with the European Union (EU), with the EU delegation setting a budget for the operationalisation of a potential EU adequacy decision.

However, others looked beyond Europe. Nigeria joined the Global Cross-Border Privacy Rules Forum as an associate member, and South Africa expressed interest in following suit. Kenya also signed the Comprehensive Economic Partnership Agreement with the United Arab Emirates, which includes



provisions to enable cross-border data flows. This signals a strategic pivot toward an alternative transfer mechanism outside the often-elusive EU adequacy framework, reflecting a broader trend among African nations to pursue diverse interoperability standards to unlock the economic value of data.

Yet this push for international interoperability has encountered significant domestic legal resistance. In a landmark ruling, the Kenyan High Court issued conservatory orders suspending the data transfer provisions of a USD 1.6 billion Health Cooperation Framework with the United States. The court acted on a petition arguing that the agreement, which facilitated the sharing of sensitive epidemiological and medical data, lacked adequate safeguards and threatened national data sovereignty. This ruling serves as a stark warning that while the executive branch may be eager to sign data-rich trade deals, the judiciary remains a formidable gatekeeper, unwilling to allow the "economic value of data" to supersede constitutional privacy rights. Similarly, regulators are increasingly targeting unauthorised data exports by international organisations. The Burkinabè government suspended two international non-profit associations for processing and transferring personal data outside the country without the required prior authorisation from the DPA. In Nigeria, the government is considering a policy proposal to require data localisation for certain categories of personal data, underscoring its intent to retain greater control over data flows.

At the continental level, the African Union Assembly of Heads of State and Government adopted the eight annexes to the African Continental Free Trade Area (AfCFTA) Protocol on Digital Trade, following the Minister of Justice's adoption in December 2024. The specific annexure on cross-border data transfer establishes a harmonised framework that mandates the free flow of data for business purposes while preserving regulatory space for privacy, effectively laying the legal rails for a unified African digital market. Also, Smart Africa mobilised 11 member states in Rabat in July to co-create Africa's first Cross-Border Data Exchange Guidelines. Under the leadership of the Council of African IT Agencies (CAITA), representatives from nations including Nigeria, Ghana, and Morocco drafted a harmonised framework to govern the interconnection of data exchange platforms.

6. The Knowledge Exchange: Building Capacity Through Collaboration

This year, the drive to address evolving challenges led DPAs to pivot from reactive regulation to proactive technical capacity building. This enthusiasm manifested in high-level collaboration, with 2025 becoming a year of intense peer-to-peer knowledge exchange. Sub-regional events surged, particularly among DPAs in the Economic Community of West African States (ECOWAS). In Senegal, the ECOWAS Knowledge Exchange convened experts from the public, private, and civil society sectors to advance regional data governance. The event focused on supporting member states with and without existing frameworks, and exploring strategies to harmonise regulations across the bloc.

Collaboration also moved beyond conferences to direct 'twinning', peer exchange, and study tours. South Africa opened its doors to Uganda's PDPO and Eswatini, while Kenya's ODPC hosted the Ugandan PDPO for a strategic benchmarking visit to share insights on implementation strategies and cross-border enforcement. Senegal extended similar hospitality to Togo, Nigeria consolidated its position as a regional learning hub, hosting officials from Botswana, Eswatini, The Gambia, Mozambique, Sierra Leone, Somalia, Tanzania, and Uganda. Meanwhile, Nigeria and Zambia announced plans to sign a memorandum of understanding on data protection to facilitate coordinated enforcement and capacity building. This engagement extended globally: Kenya's DPA conducted study tours with its counterpart in Belgium, and Nigeria's DPA visited France's CNIL in November 2025. Uganda also engaged with the European Data Protection Supervisor. In a significant move for regional leadership, Zimbabwe's DPA was nominated by the Southern African Development Community (SADC) to lead data protection capacity-building across the region. This shift toward "regulatory twinning" and global exchange signifies a transition from symbolic diplomacy to operational integration, ensuring that African authorities not only harmonise their standards locally but also align with global best practices.

7. AI Governance: From Consensus to Codification

The narrative on Artificial Intelligence in Africa shifted decisively in 2025. The year began with a push for continental consensus at the inaugural Global AI Summit on Africa in Kigali in April, where countries adopted the Africa Declaration on AI. The declaration commits member states to harmonise national AI governance frameworks and supports the newly constituted Africa AI Council, signalling a clear intent to avoid regulatory fragmentation. This was strengthened by the finalisation of the AfCFTA Protocol on Digital Trade, which includes a dedicated Emerging Technologies Annexure designed to harmonise cross-border AI standards and data flows. This continental push helps build a unified "African Voice" that could address regulatory fragmentation and ensure the continent is a rule-maker, rather than just a rule-taker, in global tech diplomacy.

The African Union and several countries also joined global AI governance initiatives. Representatives from the African Union, alongside international partners, adopted the Statement on Inclusive and Sustainable AI for People and the Planet, committing to equitable AI development and environmental sustainability in AI deployment. Kenya, Morocco, and Nigeria joined the other seven countries in signing the Paris Charter on AI in the public interest, establishing shared principles for AI governance prioritising societal benefit and human rights protection. Kenya, Nigeria, and Rwanda participated in the Seoul Declaration on Commitments to Address Severe AI Risks and the Bletchley Declaration on AI Safety. As a member of BRICS, South Africa signed the Statement on Global Governance of Artificial Intelligence, which aims to strengthen cooperation among the Global South on AI policy.

Following this high-level consensus, countries pursued a dual track of innovation-first strategies and risk-mitigating regulation. Côte d'Ivoire, Kenya, Libya, and Nigeria adopted their national AI strategies; Egypt updated its AI Strategy and announced plans to establish a dedicated body. Guinea validated its ten-year national AI roadmap (2026–2035) in partnership with the UNDP, becoming the first francophone country to adopt the Artificial Intelligence Landscape Assessment methodology. Mauritius established an AI Unit within its ICT Ministry to implement its Digital Transformation Blueprint, and Chad appointed a head to lead its newly created Directorate of Artificial Intelligence, signalling a high-level commitment to steering national AI adoption. The Moroccan government also announced plans to establish a General Directorate for Artificial Intelligence. Malawi's MACRA and Nigeria's NDPC announced plans for regulatory AI sandboxes—controlled environments for testing privacy-preserving tech. These strategic frameworks are critical because they provide the administrative infrastructure necessary to balance economic growth with ethical safeguards before binding laws are fully enacted.

However, the most significant shift was the rapid move toward binding legislation. Angola published a robust draft AI Law to establish a legal framework that prioritises ethical use, transparency, and human intervention, while categorising systems by risk level, including critical and biometric AI. The bill outlines comprehensive user rights, including the right to object to automated decisions, and imposes strict obligations on developers regarding security and content moderation. Notably punitive, it stipulates severe sanctions for non-compliance, ranging from fines of up to 15 times the national minimum wage to prison terms of up to 12 years. Similarly, the proposed amendment to the Data Protection Law also includes AI-specific provisions to ensure data protection considerations are factored into deployment, development, and use. Nigeria emerged as one of the most active jurisdictions, introducing a complex suite of bills. In February, it presented the Digital Sovereignty, AI Governance, and Fair Compensation Bill, which proposes a Digital Services Tax and data localisation mandates. This was followed by the National Artificial Intelligence Commission Bill. Most notably, the National Digital Economy and E-Governance Bill positions the National Information Technology Development Agency as a "super-regulator" with powers to classify AI risks, mandate transparency, and accredit AI auditors. Additionally, the Nigerian Communications Commission draft Internet Code of Practice includes rules governing the deployment of AI and other emerging technologies by telecommunications and internet service providers.

Ghana took a broader approach with its Emerging Technologies Bill. Rather than a standalone AI law, this bill proposes an Emerging Technologies Agency to enforce cross-functional compliance, while also allowing domain-specific regulators a role. It introduces a voluntary registration system with incentives for startups, alongside strict local content requirements capping non-local equity at 50%. The Emerging Technologies Agency would be empowered to issue policies to promote adoption and research in AI, blockchain, IoT, cloud, and quantum computing. The bill also sets rules for safe and efficient deployment, guided by principles of transparency, human oversight, bias prevention, consumer consent, and the control of misinformation. Additional proposals include the National Communications Authority Act, which would allow pre-licensing approval for AI-driven telecom services, and a Cybersecurity (Amendment) Bill, which would expand the Cyber Security Authority's powers to set standards for emerging technologies, including AI.

Morocco's Parliament is also deliberating on the Law Regulating the Use of AI. It establishes design and testing requirements for AI systems before market deployment, prohibits certain high-risk AI applications, and authorisation procedures for specified AI services. Additional provisions address data protection, content moderation for AI-generated content, and copyright regulations governing AI-generated intellectual property. Other countries are also moving toward codification. Kenya saw a Member of Parliament announce plans to introduce an AI law to address regulatory gaps, while Eswatini, Mauritius and Namibia are finalising their respective AI draft laws. With multiple bills advancing in parliaments, the race to enact Africa's first dedicated AI law is underway, and we may see one in Q2 of 2026. The move toward "hard-law" codification signifies that African regulators no longer view AI ethics as a voluntary choice, but as a high-stakes compliance requirement backed by the full force of criminal and administrative law. The imminent arrival of binding AI laws means companies must begin to operationalise a governance program framework to avoid costly retrofitting later. Also, while this transition provides the necessary "teeth" for enforcement, it also signals a risky shift toward rigid, technology-specific mandates that may struggle to remain relevant as AI capabilities evolve faster than the legislative process can keep pace.

Complementing these legislative efforts is the development of sector-specific policies and targeted regulatory warnings. The Senegalese Personal Data Protection Commission issued a significant advisory warning against the misuse of AI-generated content, specifically targeting deepfakes, identity theft, and the exploitation of personal data. This mirrors the Mauritius Financial Services Commission's stance, which published guidelines on AI in the financial sector. Tanzania has also reached advanced stages of this implementation cycle; the Ministry of Communication and Information Technology announced it is finalising a national guideline for the responsible and effective adoption of AI. Lesotho published its draft National AI Policy and Implementation Plan, which has been validated. Tanzania is finalising a national guideline for the responsible and effective adoption of AI. Uganda and Zimbabwe are also developing their AI policies, while South Africa is looking to finalise its AI policy. The significance of these advisories and soft-law guidelines is that they provide immediate, actionable guardrails for citizens and businesses, filling the critical gap between high-level legislative intent and the daily reality of digital interactions.

8. The Sovereignty Shift: Localising Data Policies

Sovereignty and strategy intersected as countries increasingly sought to domesticate continental frameworks. Kenya advanced its data governance agenda by kicking off the formulation of its National Data Governance Policy and publishing an updated Cloud Policy. This cloud framework provides guidance on adoption, supports AI, reinforces data protection principles for cross-border flows, and requires that government data be stored and processed within Kenya's territorial boundaries. Ghana also published the draft Data Protection Act, 2025, which would require domestic storage of data critical to national security, civil registration, or sensitive personal information, including children's, biometric, health, and genetic data. Morocco issued the data classification guide, setting standards for categorising data by sensitivity, with sensitive data requiring enhanced protection, including mandatory domestic storage. Rwanda published its National Data Sharing Policy and complementary data governance instruments. Egypt published its Open Data Policy, which establishes a framework to unlock public-sector data to drive innovation and transparency, positioning government datasets as a strategic asset for the digital economy.

To sustain this momentum, the African Union held a workshop to accelerate the implementation of the AU Data Policy Framework, during which stakeholders reviewed preliminary frameworks. Mozambique's National Institute of Information and Communication Technology validated the National Data Governance Policy, Strategy, and Action Plan, developed in partnership with AUDA-NEPAD and the EU. The policy aligns with the AU framework and is now a core constitutional priority in the country's digital transformation agenda. Burundi officially validated its first National Data Governance Strategy with support from UNECA, aligning with the AU framework to advance digital sovereignty. Cabo Verde also joined the strategic wave, initiating the development of its National Data Strategy with a specific focus on harnessing data in the age of AI. Similarly, the Democratic Republic of Congo, Ethiopia, Liberia, Somalia, and Sierra Leone are actively developing their national data strategies. The Gambia validated its National Data Policy to govern data management and use, and Mauritius finalised its National Data Strategy, which covers data sharing, governance, and protection. Kenya also launched consultations on ratifying the Malabo Convention, signalling a renewed commitment to the continent's foundational cybersecurity and data protection treaty. This trend marks a decisive evolution from reactive data protection to proactive data governance, treating data as a sovereign economic asset that demands a national master plan.

9. Child Online Protection

Protecting children online has shifted from a corporate social responsibility initiative to a hard compliance requirement, driven by global and regional consensus on child safety. Regional efforts showed a move toward international synchronisation. South Africa's Information Regulator joined ten other global authorities in signing a joint statement on a common international approach to age verification, reinforcing the need for strict identity checks. Similarly, Senegal and Togo participated in the launch of the Paris Peace Forum Global Coalition to Safeguard Children in the Age of AI, which aims to develop evidence-based guidelines for AI systems that affect youth. This global integration extended to technical cooperation, with Chad engaging the International Telecommunication Union (ITU) and Namibia partnering with UNICEF. The relevance of this global alignment lies in its ability to prevent "regulatory havens," ensuring that children across the continent receive a uniform standard of protection regardless of where a service provider is headquartered.

At the national level, the regulatory net tightened. Ghana reinforced its commitment by establishing a new Child Online Protection Department within the National Cyber Security Centre to address internet risks, particularly those affecting girls, supported by security awareness programs for students and teachers. Zimbabwe validated its child online policy, while Zambia launched a National Child Online Protection Strategy (2025–2029). Tunisia launched a National Charter grounded in prevention and partnership, while Mali launched the Child Protection Information Management System Plus (CPIMS+), a data-driven platform to enhance the identification and monitoring of vulnerable children. Eswatini also strengthened its institutional approach through high-level partnerships. The Ministry of ICT partnered with the Eswatini Communications Commission (ESCCOM) to bolster national cyber resilience and, concurrently, with the Deputy Prime Minister's Office to drive parental education campaigns. These strategic frameworks are critical because they move child safety from abstract legal theory into functional state operations, providing the specialised resources needed to monitor rapidly evolving digital risks.

Beyond policy frameworks, the regulatory net tightened through new and proposed legislation. Kenya enacted the Computer Misuse and Cybercrimes (Amendment) Act, which gives courts the power to order the removal of digital content and the closing of computer systems in connection with child sexual abuse material, among others. In a significant move, the Nigerian House of Representatives passed the Child Online Access Protection Bill to establish a framework to enhance digital safety. Ghana also introduced the Electronic Transactions Bill, which would require service providers that target or are likely to be accessed by children to implement age-verification mechanisms and prohibit targeted advertising based on children's personal information. Very large online platforms and search engines with around 45 million monthly users and significant influence over online content would be subject to additional obligations, including annual risk assessments and semiannual transparency reports on content moderation, automated tools, and algorithmic operations. Kenya's Communications Authority published Industry Guidelines for Child Online Protection and Safety, mandating "safety by design." Additionally, the Nigerian Communications Commission issued the draft Internet Code of Practice, including measures on online safety for minors. It requires internet access service providers to implement child protection policies, default opt-in parental controls, and multilingual safety guidance. This legislative and regulatory trend signals a shift toward "proactive accountability," in which the burden of proof shifts from parents to platforms to demonstrate that their digital environments are inherently safe for minors.

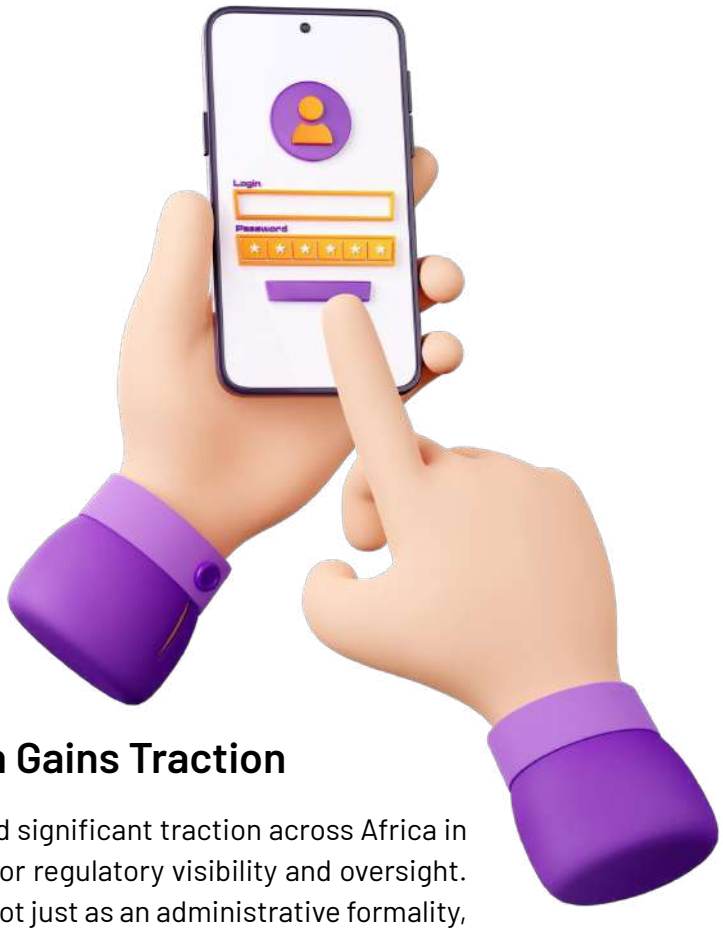
Enforcement bodies were equally active. In Mauritius, the Data Protection Office issued an urgent notice following the unauthorised disclosure of student passport details on social media, reminding the public that such actions attract fines of up to 200,000 rupees (approximately USD 434) and imprisonment. Similarly, in Uganda, the PDPO ordered a school to delete a post on X (formerly Twitter) featuring children's images. The PDPO emphasised that the post violates the provisions of the Data Protection and Privacy Act and poses significant risks to the children. The post was taken down in compliance with the directive. In Tanzania, the Personal Data Protection Commission issued a decision strictly prohibiting the unauthorised use of children's images and strengthening consent requirements for minors. Kenya's ODPC further underscored this punitive trend by fining a hair manufacturing company KES 700,000 (approximately USD 5,430) for using a minor's image on social media for commercial marketing without parental consent. The Commissioner ruled that the company's reliance on the minor's oral assertion that they were over 18 was legally ineffective, emphasising the statutory duty of data controllers to implement robust age-verification and consent mechanisms. In South Africa, the Film and Publication Board (FPB) briefed Parliament on the challenges posed by "misaligned platform standards" and committed to issuing takedowns and monitoring digital activity more aggressively. Additionally, the FPB ordered the takedown of online content depicting violence against children, and reported on investigations into the distribution of online child sexual abuse material on digital platforms. Meanwhile, there is a growing advocacy for an "Australia-esque" ban on social media for children, highlighting that existing legal regimes were insufficient to curb rising online abuse. The significance of these enforcement actions is that they provide the "teeth" necessary for data protection laws to function, demonstrating to both public and private entities that violations of children's privacy will result in immediate and tangible legal consequences.

10. National Cybersecurity Frameworks Solidify

A defining trend across the continent in 2025 was the acceleration of the adoption of comprehensive cybersecurity frameworks, reflecting a clear recognition that Africa's digital transformation cannot advance without robust protection against cyber threats. Governments moved aggressively to enact laws and establish institutions to secure critical infrastructure and manage incident response. In Angola, the Ministry of Telecommunications, Information Technology and Media took decisive steps by calling for comments on a proposed cybersecurity law, a law on the dissemination of fake news, and a national cybersecurity strategy. This legislative push culminated in December, when Angola issued two presidential decrees approving the National Cybersecurity Strategy and establishing the National Cybersecurity Centre as an autonomous public institute with regulatory and sanctioning powers to oversee the country's cyber resilience.

Kenya's Ministry of Interior and National Administration published the revised draft of the National Cybersecurity Strategy (2025-2029) for public comment, emphasising the integration of AI and a harmonised approach to incident response. South Sudan's National Legislative Assembly passed the Cybercrime and Computer Misuse Bill, 2025, which establishes a dedicated national cybercrime department within the Ministry of Justice. Similarly, Djibouti presented a bill to its Parliament to establish the National Cybersecurity Authority to safeguard national cyberspace and build investor confidence. Liberia's Parliament passed the Cybercrimes Act 2025, which expands the functions of the Liberia Computer Emergency Response Team and criminalises offences such as identity intrusion. Botswana's Parliament deliberated on the draft Cybersecurity Bill to strengthen the institutional framework for protecting critical information infrastructure. Meanwhile, the Malagasy Government formally launched the process to develop its national cybersecurity strategy to improve coordination between public institutions and private-sector actors. South Africa's Information Regulator contributed its official position on a bill to establish the Office of the Cyber Commissioner, which would be responsible for maintaining cybersecurity capabilities and managing an incident-reporting hub.

Complementing domestic reforms, African countries steadily aligned themselves with international norms to ensure interoperability. Rwanda acceded to the Budapest Convention. In a significant move toward global cooperation, 21 African countries signed the United Nations Convention against Transnational Organised Crime. Simultaneously, the African Union is exploring mechanisms to support member states in adopting this convention, addressing the significant operational and legal challenges required for its implementation. Regional bodies, including the Intergovernmental Authority on Development, actively encouraged harmonised cybersecurity approaches to address growing cross-border risks. These developments underscore a continent-wide shift from reactive measures to a proactive, institutionalised cyber defence architecture.



11. Mandatory Registration Gains Traction

The trend of mandatory registration gained significant traction across Africa in 2025, serving as the primary mechanism for regulatory visibility and oversight. Regulators increasingly view registration not just as an administrative formality, but as the foundational step for enforceability and accountability. In Kenya, the ODPC issued strict reminders to data controllers and processors to register, emphasising that visibility is a key step in ensuring compliance. Similarly, Mauritius' Data Protection Office (DPO) mandated all entities processing personal data to register, explicitly warning that failure to comply could result in severe penalties, including fines or imprisonment. Reminders were also prominent in Ghana, Eswatini, Nigeria, Rwanda, Tanzania, and Uganda.

Regulators in other jurisdictions introduced tiered and sector-specific registration requirements. Malawi's MACRA initiated the registration process for "Data Controllers and Processors of Significant Importance", establishing a six-month compliance window starting April 1, 2025. In Tanzania, the PDPC integrated compliance reporting with registration by beginning to submit quarterly reports and DPIAs through its registration system. Nigeria's NDPC reinforced accountability by reminding data controllers and processors to register with it.

Enforcement of these requirements is becoming increasingly rigorous. Eswatini's (EDPA announced the renewal of registration licences for some controllers and urged all entities to ensure continued compliance. Crucially, the EDPA announced that from September 2025, it would initiate enforcement actions against all organisations that failed to comply with registration requirements following the conclusion of the registration process. Ghana's DPC also urged data controllers and processors to register with it. This continent-wide tightening of registration protocols signals that regulators are closing the net on unregistered entities, making regulatory visibility the non-negotiable price of doing business in Africa's digital economy.

12. The Convergence of Competition and Data Protection

Finally, the intersection between competition and data protection was further blurred. In December, COMESA adopted new Competition and Consumer Protection Regulations that explicitly list "data quantity and control" as factors for determining market dominance. This "Gatekeeper" regulatory style, banning dark patterns and mandating portability, signals that, for African regulators, data accumulation is now a measure of market power. The Commission's powers have expanded to include "dawn raids," signalling an aggressive stance.

Supporting this regional move, the COMESA Competition Authority issued an advisory on data protection and signed a Memorandum of Understanding with the East African Community Competition Authority to facilitate information sharing during joint investigations. At the national level, South Africa's Competition Commission published a Draft Guidance Note for Online Intermediation Platforms that directly targets how platforms use non-public data to compete against their own business users, defining such practices as "unfair treatment." The Competition Commission also published the final report of its Media and Digital Platforms Market Inquiry, which assessed market concentration, data advantages, and potential anticompetitive practices in media and digital platforms. The report notes that local news media face challenges from global platforms, declining advertising revenue, and limited subscriptions, and notes issues such as reduced referral traffic, use of data for AI without compensation, and algorithmic prioritisation. Recommendations include a ZAR 688 million Media Support Package, expanded publisher contracts, increased AdTech transparency, and measures for AI content management. Further, the Nigerian Federal Competition and Consumer Protection Tribunal upheld the Commission's ruling that the data-sharing practices of a global social media entity were anticompetitive. This decision reinforces the Commission's regulatory authority over digital service providers and sets a precedent for applying competition law to data-driven business models. This convergence signifies a fundamental shift in African governance, in which data is no longer treated solely as a private asset but as critical infrastructure for market power, requiring aggressive competition oversight to ensure fair digital competition.

Part II:

Predictions for 2026

As we look toward 2026, the foundational work of 2025 sets the stage for a year of harmonisation, rigorous sector-specific regulation, and the expansion of the African data protection map.

1. We expect the enactment of new laws in Liberia, Mozambique, Namibia, Sierra Leone, and South Sudan. We also expect to see progress in amendments to laws in Angola, Ghana, Nigeria, Senegal, and other countries.

2. In addition to new laws, we would see the creation of designation of new DPAs. Countries with laws but without DPAs are also expected to operationalise their law.

3. We anticipate the enactment of the first dedicated AI laws on the continent before the end of the second quarter. Nigeria's National Digital Economy Bill is expected to be signed into law in Q2 2026, creating a comprehensive "super-regulator" framework. Elsewhere, Angola, Morocco, and Namibia remain frontrunners, but Kenya may also accelerate the introduction of an AI Bill.

4. Enforcement from DPAs is expected to increase, and domain and sector-specific regulators are expected to impose data protection-related sanctions. The era of the "administrative fine" as the sole deterrent is gradually coming to an end. Following the two criminal convictions in Uganda and the prison sentence in South Africa, we anticipate more criminal convictions for data protection offences. This will be supported by greater cross-border collaboration among regulators. We expect to see more joint investigations.

5. We expect to see an increase in litigation and representative actions brought by civil society organisations and individuals against government agencies and private companies for different violations. We also expect to see copycat complaints to DPAs and litigation across different countries.

6. Child online safety will gain more prominence than ever before, translating legislative momentum into aggressive enforcement. We predict more fines will be levied for failing to implement child-appropriate practices. Regulators will move beyond simple content moderation to scrutinise platform architecture and the "sharenting" practices of minors and influencers.

7. The map of permissible international data flows will be further drawn. We expect greater CBPR traction and anticipate countries publishing their own adequacy lists and providing clarity on their data transfer mechanisms, with Kenya possibly securing an EU adequacy decision. The operationalisation of the AfCFTA Digital Trade Protocol's Cross-Border Data annexure is expected to further drive a broader conversation on continental interoperability and challenge the current fragmentation of transfer rules.

8. Legislative progress will expand beyond national parliaments to the regional blocs, driving harmonisation from the top down. We expect the ECOWAS Supplementary Data Protection Act to be concluded, the development of an EAC data protection framework, and the launch of an SADC AI strategy.

9. DPAs would publish additional guidance notes and guidelines to clarify the law. Heightened scrutiny will extend to specific high-risk industries, where we predict the development of industry-specific regulations.

10. We anticipate a definitive shift toward experimental regulation. We predict the adoption of policy prototyping, with DPAs launching regulatory sandbox programmes to test compliance technologies in real time. Nigeria has already signalled this direction with the NDPC's move to create AI sandboxes, and we expect other countries to follow suit.

Conclusion

In 2025, the African data protection landscape matured. It shed its theoretical skin and emerged as a fledgling, muscular, albeit complex, regulatory environment. The "Year of the Teeth" taught us that laws are only as good as their enforcers, and African enforcers are increasingly bold, collaborative, and innovative.

As we look to 2026, the challenge for organisations will not just be "compliance" in the static sense, but "agility." With AI laws looming, competition authorities entering the privacy arena, and child safety obligations on the horizon, the only safe strategy is proactive, ethical, and deeply attuned to the local realities of the African market. For international organisations, the days of cutting and pasting "global" policies for African subsidiaries and operations are eclipsing.

TECH HIVE ADVISORY

December 2025

Digital Policy Alert

PRIVACY GUIDE AFRICA

PRIVACY LENS AFRICA

Ulinzi