ACT Association for Competitive Technology

5 June 2026

Eng. John Tanui, CBS
Principal Secretary
State Department for ICT and the Digital Economy
Ministry of Information, Communications and the Digital Economy
Telposta Towers, Koinange Street
P.O. Box 30025-00100
Nairobi, Kenya

RE: Comments of the Association for Competitive Technology on the Draft Final National Data Governance Policy (May 2026)

Dear Principal Secretary Tanui,

The Association for Competitive Technology (ACT) appreciates the opportunity to comment on the Draft Final National Data Governance Policy (the Policy) published by the Ministry of Information, Communications and the Digital Economy (MICDE) in May 2026.

I. Introduction and Statement of Interest

ACT represents micro-, small-, and medium-sized enterprise (MSME) application developers and connected device companies located both within Kenya and around the globe.[1] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. These efforts today represent an economy worth more than $1.8 trillion annually and that provides millions of jobs around the world.[2]

Kenya has become an increasingly important market for the global digital economy as digitalisation continues across the African continent. Yet this opportunity is increasingly threatened by the emergence of digital trade barriers, including data localisation mandates, restrictions on cross-border data flows, internet shutdowns, and discriminatory taxes on digital services, all of which undermine investment and limit the growth of integrated digital markets in Kenya. A modernised data governance approach in Kenya should reinforce an open and competitive digital environment that supports long-term economic engagement and digital connectivity, consistent with the Kenya Cloud Policy 2024 and its recognition of the importance of facilitating cross-border transmission, fostering interoperability, and strengthening collaboration across nations. Kenya's approach to data governance will not only shape how Kenyan innovators participate in the Kenyan digital economy, but will also serve as a model for Africa.

[1] Association for Competitive Technology, About, available at http://actonline.org/about.
[2] Association for Competitive Technology, State of the App Economy (2022), available at https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL.pdf.

ACT has engaged constructively in Kenya's digital policy development before. The comments below build on several previous submissions that ACT has made to the Kenyan government, including:

- ACT's June 2024 comments on proposed updates to the Competition Act, in which we set out the platform functions that MSMEs depend on and cautioned against transposing foreign regulatory models that have not been shown to strengthen competitiveness or to empower MSMEs.[3]
- ACT's May 2026 comments to the Office of the Data Protection Commissioner (ODPC) on its draft guidance notes on cross-border data transfers and on institutional data protection policy.[4]

We commend MICDE for recognising data as an enabler of inclusive growth, for grounding the Policy in findable, accessible, interoperable, and reusable (FAIR) principles, for the goal of reducing duplicative data requests on citizens and businesses, and for the technology-neutral framing of the emerging technologies chapter. The consultative multi-stakeholder process that produced the draft is itself a model worth sustaining as the framework moves into implementation. ACT's recommendations are offered to ensure that the framework keeps Kenya open to trusted data flows, protects the interests of MSMEs that drive competition and innovation, and protects Kenyan consumers.

II. ACT's General Views on Data Governance

ACT offers five cross-cutting themes which we urge MICDE to align with as it moves forward with establishing an updated national data governance policy:

1. **A national framework should reduce friction for the smallest innovators.** The Policy correctly observes that uniform compliance requirements can fall hardest on MSMEs.[5] Obligations that a large multinational or a well-resourced ministry can absorb may be prohibitive for a startup or a sole developer. ACT urges a risk-based and proportionate approach throughout the framework, so that obligations scale to the volume and sensitivity of the data an organisation processes and align with objective outcomes and a common taxonomy cross-walked to established standards such as ISO/IEC 27701 and other globally recognised frameworks.
2. **Trusted data flows (without data localisation) deliver the economic value the Policy seeks.** The Policy's own international experts recommended clear adequacy frameworks, avoidance of overly restrictive localisation mandates, and a tiered, risk-based approach to

[3] Association for Competitive Technology, Comments re Updates to the Kenya Competition Act (11 June 2024), available at https://actonline.org/wp-content/uploads/ACT-Comments-re-Updates-to-Kenya-Competition-Act-11-June-2024.pdf.
[4] Association for Competitive Technology, Comments on the ODPC Draft Guidance Notes on Cross-Border Data Transfers and on Institutional Data Protection Policy (15 May 2026).
[5] Draft Final National Data Governance Policy (May 2026), Section 4.3.1 (noting that uniform compliance requirements disproportionately burden smaller enterprises).

cross-border transfers.[6] Well-established evidence demonstrates that data localisation mandates raise prices for consumers, reduce competitiveness, weaken cybersecurity outcomes, and deter foreign investment without producing measurable gains. They also weigh most heavily on the MSMEs that cannot maintain in-country infrastructure in every jurisdiction in which they operate.

3. **Predictability and regulatory coherence are vital.** MSMEs and startups in particular need to know which regulator they answer to and what is expected of them. The Policy layers a new National Data Governance and Emerging Technologies Council over the ODPC, the Communications Authority, and a range of sector regulators. Clear delineation of mandates and a single point of contact for business will determine whether the framework lowers or raises the cost of compliance.
4. **Incentives and capacity support will drive compliance more effectively than mandates alone.** The Policy's experts have observed that obligations imposed without genuine incentives tend to produce low uptake.[7] Model contracts, standardised agreements, plain-language guidance, streamlined certification pathways, and reduced burdens for demonstrated good practice will do more to lift the maturity of Kenya's data ecosystem than penalties applied to firms that lack the capacity to comply.
5. **Kenya should build on experiences from other jurisdictions where comparable regimes have struggled.** The Policy benchmarks extensively against the European Union and other jurisdictions, and its experts wisely encouraged Kenya to study where approaches elsewhere have not worked. We would reinforce that caution. Several heavily prescriptive frameworks abroad have not been shown to improve competitiveness or to empower MSMEs, and importing their most burdensome features risks the costs without the benefits. Kenya is well positioned to design a framework that fits its own market and its regional integration commitments.

III. ACT's Specific Recommendations on the Draft Final National Data Governance Policy

a. Preserve trusted cross-border data flows and avoid data residency and localisation mandates.

Intervention 6.1.1 would require that critical infrastructure and strategic economic data remain in-country, while non-sensitive data would enjoy a presumption of free flow. While we support the presumption of free flow and urge that it be the default for all non-personal data, any in-country requirement should be narrowed to apply only where processing directly supports core sovereign functions. Ordinary commercial service delivery, including in sectors such as healthcare and education, should not by default be treated as processing for the strategic interest of the state. Where the framework contemplates an in-country copy of data, that obligation should be capable of being satisfied through interoperable cloud architectures and should not compel duplicative on-premises infrastructure that MSMEs cannot afford.

[6] Id., Section 2.6.5 (international data governance experts recommending clear adequacy frameworks, avoidance of overly restrictive data localisation mandates, and a tiered, risk-based approach to cross-border transfers).

[7] Id., Section 2.6.5 (experts noting that imposing additional duties on data actors without genuine incentives tends to produce low uptake, and recommending that obligations be paired with positive incentives).

Broad localisation mandates would also be inconsistent with Kenya's own commitments under the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol, which promotes cross-border data flows and disciplines unjustified localisation requirements among African Union Member States, and with the East African Community Common Market Protocol. Onerous data localisation policies also stand to undermine the ongoing United States and Kenya bilateral trade negotiations, in which open cross-border data flows and the avoidance of forced data localisation are core United States digital trade priorities, and would complicate Kenya's position as it seeks long-term preferential trade arrangements beyond the African Growth and Opportunity Act.

ACT encourages MICDE to prioritise the trust-based transfer mechanisms the Policy already references, including adequacy arrangements, reciprocal data protection agreements, binding corporate rules, contractual safeguards, the Global Cross-Border Privacy Rules system, and ISO/IEC 27701 certification as a basis for appropriate safeguards. We further encourage MICDE to coordinate with fellow African data protection authorities and the AfCFTA Secretariat to advance mutual recognition, to support Kenya's continued engagement with and consideration of formal participation in the Global CBPR Forum, and to align the cross-border provisions with the contemplated amendment to Section 48 of the Data Protection Act.

b. Defer to existing contractual and intellectual property frameworks in addressing data as a factor of production.

Intervention 3.1.1 and Section 5.2.4 propose recognising data as a factor of production and establishing default property rights based on origination, collection investment, and value-addition. ACT cautions against creating a novel statutory ownership regime in data, which would be a far-reaching step that few jurisdictions have taken and which would generate significant legal uncertainty. Data is already governed by an interlocking set of existing legal frameworks in Kenya, including contract, trade secret protection, the Copyright Act, the Industrial Property Act, and the Data Protection Act. In particular, because intellectual property and trade secret protection is critical to MSME innovation, a new layer of default ownership rights risks conflicting with those frameworks, complicating routine commercial arrangements, and chilling the very investment the Policy seeks to attract.

We respectfully recommend that the Data Governance Law clarify rights and responsibilities through existing contractual and intellectual property mechanisms, and through clear rules on access, use, and sharing, rather than by creating new property rights in data. If MICDE nonetheless proceeds, we urge a careful, separately consulted process focused narrowly on the gaps that existing law does not address, so that the framework adds clarity rather than litigation risk and does not disturb the intellectual property protections on which our members rely.

c. Keep AI and emerging-technology data governance risk-based, proportionate, and innovation-enabling.

The emerging technologies chapter of the Policy commits to principles that are technology-neutral in design and responsive in application, which we support. However, Intervention 4.1.2 would require standardised, pre-deployment risk assessments for high-impact data uses, including AI training data. For an MSME, a heavy mandatory audit applied to every model or dataset would be prohibitive. ACT recommends that such assessments be reserved for genuinely high-risk uses,

scaled to the size of the actor and the nature of the risk, and built on the foundation that KS/DKS 3007 already provides.

ACT also urges MICDE to ensure that the intellectual property rules contemplated for AI models trained on lawfully accessible public data, and any associated benefit-sharing obligations, do not require MSME developers to undertake unpredictable, lengthy, or costly negotiations with data holders before they can build or improve their products. Clear and predictable permissions to use lawfully accessible data for training, including through text and data mining, are essential if Kenyan MSMEs are to develop and compete in AI. We further encourage MICDE to ensure that obligations on AI training data and high-impact datasets do not replicate or conflict with the ODPC's existing mandate over personal data. Regulatory sandboxes, which the Policy contemplates, are an advisable tool for allowing MSMEs to test innovative data uses under supervision, and we encourage their early and generous use.

d. Calibrate compliance obligations to risk.

In the Policy, depending on the data involved, MICDE contemplates prescriptive recordkeeping and retention requirements that could run counter to other goals of the framework, including data minimisation and the right of data subjects to have their data deleted. ACT requests clear guidance on how to resolve such conflicts, and the establishment of de minimis thresholds that exempt the smallest MSMEs from the most resource-intensive requirements, simplified pathways for low-risk processing, and the provision of free model contracts, templates, and standardised data-sharing agreements. The Policy's experts specifically endorsed model contracts and standardised agreements as a way to reduce transaction costs and protect MSMEs against exploitative terms from larger data holders. Embedding these tools in the framework, and resourcing the capacity-building programmes the Policy describes, would make compliance achievable for the MSMEs that most need support.

e. Keep data intermediary and marketplace frameworks light-touch, interoperable, and voluntary.

Interventions 3.1.2 and 6.2.2 would license and regulate data marketplaces and require registration of data intermediaries, brokers, and marketplace operators. ACT cautions MICDE that licensing and registration regimes can become barriers to entry for MSMEs and startups that often drive innovation. We recommend that any such regime be light-touch and proportionate, that participation in marketplaces be voluntary, and that the framework prioritise open standards and interoperability so that MSME participants are not locked into a single operator.

f. Preserve the ability to use strong encryption.

The Policy contemplates role-based security and encryption guidelines and post-quantum cryptography readiness, which ACT supports. Strong encryption is essential to protecting end users from harms such as identity theft and to maintaining the trust on which digital products and services depend. We encourage MICDE to affirm support for strong, modern encryption and to avoid any requirement that providers build backdoors or guaranteed government-access mechanisms into encryption. Such mandates create known vulnerabilities that unauthorised parties can exploit, and they weaken the security outcomes the Policy seeks to advance.

g. Address competition concerns through competition law, not the data governance framework.

Intervention 6.2.2 would embed rules aimed at preventing dominance through data hoarding. ACT shares the goal of competitive data markets, but we caution against importing untested platform competition theories into the data governance framework. Competition matters are best addressed by the Competition Authority of Kenya under existing competition law, applied to evidence of actual harm, rather than through ex ante rules placed in a data governance instrument. As ACT noted in its 2024 comments on the Competition Act, prescriptive frameworks borrowed from abroad have not been shown to strengthen competitiveness or to empower MSMEs.

h. Ensure institutional coherence and avoid duplicative or conflicting mandates.

The Policy and the proposed Data Governance Law would establish the National Data Governance and Emerging Technologies Council alongside the ODPC, the Communications Authority, and sector regulators. We encourage MICDE to define each body's mandate precisely, to establish clear coordination mechanisms, and to provide businesses with a single front door for data governance questions. Overlapping or conflicting guidance from multiple regulators is a particular hardship for MSMEs that lack dedicated compliance staff. We also note that guidance and subsidiary instruments should not expand the obligations established by primary legislation.

i. Advance interoperability through open, international, and vendor-neutral standards.

ACT supports the Policy's emphasis on interoperability, open standards, the FAIR principles, and an API-first approach. These are the features of the framework most likely to benefit MSMEs, because they lower the cost of building on public infrastructure and reduce dependence on any single vendor. We encourage MICDE to anchor the national interoperability guideline and the national API gateway in open, internationally recognised standards, and to avoid mandating specific architectures or technologies that could disadvantage MSME vendors or foreclose future innovation. Vendor-neutral procurement, which Intervention 1.1.1 contemplates, is an important safeguard against the lock-in that the Policy rightly identifies as a problem.

j. Pair obligations with incentives and provide a realistic implementation runway.

The Policy contemplates commencement in July 2026 through a phased approach. We encourage MICDE to confirm that timelines for any new obligations are realistic, that subsidiary legislation and technical standards are themselves subject to public consultation, and that businesses receive adequate notice and transition periods before new requirements take effect. Pairing obligations with the incentives the Policy's experts recommended, including financial support, recognition and certification schemes, and reduced burdens for good practice, will improve uptake far more than enforcement alone.

IV. Conclusion

ACT shares MICDE's ambition to make data a driver of inclusive growth and to position Kenya as a leader in Africa's digital economy. The surest path to that goal is a framework that the smallest innovators can navigate, that keeps Kenya open to trusted data flows and regional integration, that protects the intellectual property and encryption-based security that MSMEs rely on, that relies on existing legal tools rather than untested new ones, and that pairs proportionate obligations with real support and incentives.

We would welcome the opportunity to discuss these comments further and to serve as a resource as MICDE develops the Data Governance Law and its implementing measures. Thank you for considering our views.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

Association for Competitive Technology

Comments of the Association for Competitive Technology (ACT)
on the Draft Final National Data Governance Policy (May 2026)

Name of organisation: Association for Competitive Technology (ACT)
Contact: Brian Scarpelli, (Senior Global Policy Counsel) and Chapin Gregor (Policy Counsel)
Email / Telephone: bscarpelli@actonline.org | +1 517-507-1446
Date: 5 June 2026

No.	Policy section / intervention	Provision as drafted	ACT recommendation	Justification
1	Principle 3.3(d) (Data sovereignty) and Intervention 6.1.1	Asserts a sovereign right to govern all data generated in Kenya and would require critical infrastructure and strategic economic data to remain in-country, with free flow only for non-sensitive data.	Make a presumption of free flow the default for all non-personal data. Narrow any in-country requirement to processing that directly supports core sovereign functions, and confirm that ordinary commercial service delivery (including healthcare and education) is not by default a strategic state interest. Allow any in-country copy to be met through interoperable cloud rather than duplicative on-premises infrastructure. Prioritise adequacy, binding corporate rules, contractual safeguards, the Global CBPR system and ISO/IEC 27701, pursue mutual recognition with the AfCFTA Secretariat and African data protection authorities, and align with the Section 48 DPA amendment.	Localisation raises consumer prices, reduces competitiveness, weakens cybersecurity, and deters investment without measurable gains, and falls hardest on MSMEs. Broad localisation conflicts with the AfCFTA Digital Trade Protocol and the EAC Common Market Protocol, and risks the ongoing US-Kenya trade negotiations and Kenya's pursuit of preferential arrangements beyond AGOA.
2	Intervention 3.1.1 and Section 5.2.4 (data as a factor of production)	Would recognise data as a factor of production and create default property rights based on origination, collection investment, and value-addition.	Do not create a novel statutory ownership regime in data. Clarify rights through existing contract and intellectual property mechanisms and clear rules on access, use, and sharing. If MICDE proceeds, consult separately and target only the gaps existing law does not address.	A new ownership regime generates legal uncertainty and conflicts with contract, trade secret protection, the Copyright Act, the Industrial Property Act, and the Data Protection Act, complicating routine commercial arrangements and chilling investment. Intellectual property and trade secret protection is critical to MSME innovation.
3	Interventions 4.1.2, 4.4.2 and 6.2.1 (AI and emerging technologies)	Would require standardised, pre-deployment risk assessments for high-impact data uses including AI training data, and contemplates	Reserve pre-deployment assessments for genuinely high-risk uses, scaled to actor size and risk, and built on KS/DKS 3007. Ensure intellectual	Heavy mandatory audits and licensing or benefit-sharing burdens are prohibitive for MSME AI

No.	Policy section / intervention	Provision as drafted	ACT recommendation	Justification
		intellectual property rules and benefit-sharing for AI models trained on public data.	property rules and benefit-sharing obligations for AI models trained on lawfully accessible public data do not force MSME developers into unpredictable, lengthy, or costly negotiations with data holders. Provide clear, predictable permissions to use lawfully accessible data for training, including through text and data mining. Avoid duplicating the ODPC's personal-data mandate, and use regulatory sandboxes generously.	developers and would deter AI development in Kenya, while clear training-data permissions enable MSMEs to build and compete.
4	Interventions 1.1.1 to 1.1.5 and 3.2.1 (DGIAs), and recordkeeping and retention	Imposes documentation, data-asset-register, data-mapping, Data Governance Impact Assessment, and recordkeeping obligations across actors of all sizes.	Adopt a risk-based, proportionate approach cross-walked to ISO/IEC 27701. Scale obligations to business size and complexity, set de minimis thresholds for the smallest MSMEs, provide simplified pathways for low-risk processing, and supply free model contracts, templates, and standardised data-sharing agreements. Give clear guidance where recordkeeping and retention conflict with data minimisation and deletion rights.	The Policy itself notes that uniform requirements burden smaller enterprises (Section 4.3.1). MSMEs lack dedicated compliance departments, and overly prescriptive requirements may push them out of the Kenyan market. Model contracts reduce transaction costs and protect MSMEs from exploitative terms.
5	Interventions 3.1.2 and 6.2.2 (data intermediaries and marketplaces)	Would license and regulate data marketplaces and require registration of data intermediaries, brokers, and marketplace operators.	Keep any regime light-touch, proportionate, and voluntary, and prioritise open standards and interoperability so that MSME participants are not locked into a single operator.	Licensing and registration can become barriers to entry that favour incumbents and exclude the MSMEs and startups that drive innovation. Transparency and accountability for high-impact data can be achieved without a heavy authorisation process.
6	Intervention 1.1.1(h) and Intervention 4.2.1 (security and post-quantum cryptography)	Contemplates role-based security and encryption guidelines and post-quantum cryptography readiness.	Affirm support for strong, modern encryption and avoid any requirement that providers build backdoors or guaranteed government-access mechanisms into encryption.	Strong encryption protects end users (for example from identity theft) and underpins trust in digital products and services. Access mandates create known vulnerabilities that unauthorised parties can exploit and weaken the security

No.	Policy section / intervention	Provision as drafted	ACT recommendation	Justification
				the Policy seeks to advance.
7	Intervention 6.2.2 (fair competition rules)	Would embed fair competition rules aimed at preventing dominance through data hoarding.	Address competition concerns through the Competition Authority of Kenya under existing competition law, on evidence of actual harm, rather than through ex ante rules placed in a data governance instrument.	Importing untested platform competition theories into a data law creates uncertainty. As ACT noted in its 2024 Competition Act comments, prescriptive borrowed frameworks have not been shown to strengthen competitiveness or to empower MSMEs.
8	Sections 4.2, 5.1 and 5.2.4 (institutional coordination)	Establishes the National Data Governance and Emerging Technologies Council alongside the ODPC, the Communications Authority, and sector regulators.	Define each body's mandate precisely, establish clear coordination mechanisms, and provide businesses with a single front door for data governance questions. Ensure guidance and subsidiary instruments interpret, rather than expand, primary legislation.	Overlapping or conflicting guidance from multiple regulators is a particular hardship for MSMEs that lack dedicated compliance staff.
9	Interventions 1.1.1 and 1.1.5, and FAIR principles (interoperability)	Commits to interoperability, the FAIR principles, an API-first approach, and a national API gateway.	Anchor the national interoperability guideline and the API gateway in open, internationally recognised, vendor-neutral standards, and avoid mandating specific architectures or technologies that disadvantage MSME vendors. Maintain vendor-neutral procurement (Intervention 1.1.1).	ACT supports these features as the most beneficial to MSMEs, because they lower the cost of building on public infrastructure and reduce dependence on any single vendor.
10	Section 5 (commencement July 2026)	Phased implementation commencing July 2026.	Confirm that timelines are realistic, subject subsidiary legislation and technical standards to public consultation, provide adequate notice and transition periods, and pair obligations with incentives such as financial support, recognition and certification schemes, and reduced burdens for good practice.	Incentives drive uptake more effectively than penalties, and a predictable, well-sequenced rollout allows MSMEs to plan and invest with confidence.