# *CIPESA Submission on the Draft Guidance Note on Artificial Intelligence*

**August 2026**

**Name of the Entity: The Collaboration on International ICT Policy for East and Southern Africa (CIPESA)**

**Name of the Guidance Note: Draft Guidance Note on Artificial Intelligence**

August 17, 2026

The Compliance Directorate
Office of the Data Protection Commissioner (ODPC)
Britam Towers 12th Floor, Hospital Road, Upperhill, Nairobi, Kenya.
P.O Box 30920-00100 G.P.O Nairobi, Kenya
By email: compliance@odpc.go.ke

Dear Sir/Madam,

**RE: SUBMISSION ON THE DRAFT GUIDANCE NOTES ON ARTIFICIAL INTELLIGENCE**

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) welcomes the opportunity to comment on the Guidance Notes on Artificial Intelligence published for public participation by the Office of the Data Protection Commissioner (ODPC). Thank you for the great work that you are doing to shape data protection and governance in Kenya and the entire region. Following the call for comments on the three Guidance Notes on Artificial Intelligence, Emerging Technologies and Privacy Enhancing Technologies, as a means to provide clear and concise guidance on the handling of personal data in accordance with the law in Kenya, CIPESA hereby submits its comments on the Guidance Note on Artificial Intelligence for your consideration.

We welcome the opportunity to discuss any part of this submission with the office.

Yours sincerely,

CIPESA Team

| No. | Page No. & Section of Guidance Note | Statement as currently captured | Proposed Statement | Comments/Justification |
|---|---|---|---|---|
| 1. | **(Page 9-11) on Legislative Framework** | Captures only national laws, sections 3 (a) – (f) | Add section 3(g) recognising African instruments:<br>1. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). Provides a framework for fostering trusted, secure, and unified digital ecosystems across Africa to enhance trade and economic growth, facilitate them, and protect the right to privacy.<br>2. AU Data Policy Framework. Aims to harmonise and strengthen data governance frameworks in Africa. It aims to facilitate the seamless flow of data across the continent for social, economic, and digital transformation<br>3. AU Continental AI Strategy. A continental instrument which aims to foster an integrated Africa that is prosperous and driven by responsible use and application of AI. It is also an instrument that could potentially steer inclusive growth, technological development and innovation in accordance with Agenda 2063. | These instruments, alongside others, provide for harmonisation of data governance on the continent. It would be absurd to leave them out as part of the legislative framework guiding AI systems in Kenya. Indeed, it would place Kenya as one of the countries not heeding regional data governance frameworks.<br><br>Kenya has not yet ratified the Malabo Convention; the Guidance Note should describe accession as "in progress" rather than assume completed ratification. |
| 2. | (Page 22) Section 7.9 on Cross-Border Transfers of AI-Processed Data | Para 2: "Entities shall assess and document the adequacy of data protection in any jurisdiction to which personal data is transferred in connection with AI processing and shall implement contractual or<br>other safeguards including binding corporate rules or contractual clauses where adequacy cannot be established. Entities may not | Retain the adequacy and safeguards requirement, but add: "Entities shall take into account applicable African regional and continental frameworks, including the AU Data Policy Framework and the African Continental Free Trade Area (AfCFTA), when assessing cross-border transfers of personal data processed through AI systems, within the contractual clauses and adequacy standards and mechanisms aligned with while maintaining appropriate data protection safeguards." | The paragraph in its current state risks the unwarranted application of blanket data localisation, which poses risks of friction in cross-border AI inference and cloud compute capabilities. It is imperative to harmonise cross-border data flows in accordance with the AU Data Policy Framework and the AfCFTA Protocol on Digital Trade. This will bring the provision in harmony with the core 1 and 4 of the AU Continental AI Strategy. |

| | | | | |
|---|---|---|---|---|
| | | transfer personal data to offshore AI processors without a lawful transfer basis." | | It should address cases such as Worldcoin, where a foreign company processed and exported "iris data" without a DPIA.<br><br>It will also put a check on possible and potential market fragmentation, hindrance of intra-African digital trade, and the risks posed to privacy protection on the continent. |
| 3. | (Page 28) Section 9 (Table, row 4, columns 1 to 3)<br><br>"AI-Enabled Biometric Recognition (Facial, Fingerprint, Voice)" | "DPIA required; Explicit consent or statutory basis; DPO mandatory; strict access controls; prohibition on real-time biometric surveillance absent specific legal authority" (specific obligations) | "DPIA required; Explicit consent or statutory basis; DPO mandatory; strict access controls; prohibition on real-time and retrospective biometric surveillance absent specific legal authority; mandatory pre-deployment registration and DPIA submission to the Office before biometric data collection begins, consistent with the deficiencies identified in the Worldcoin case. | Since biometric data is Sensitive Personal Data (Section 2 of the Data Protection Act), retrospective biometric surveillance (e.g., searching stored facial or iris data after the fact) poses an equal risk of mass surveillance that imposes a chilling effect on constitutional rights and freedoms, including expression, assembly and privacy.<br><br>The Worldcoin case demonstrates that reactive enforcement (after data has already been collected from hundreds of thousands of people) is a weak remedy; a pre-deployment is a stronger and more proportionate safeguard. |
| 4. | (Pages 30-31) Generative AI | (c) ensure that appropriate safeguards are implemented to reduce the risk of hallucinations, inaccurate personal information, or misleading outputs concerning identifiable individuals, particularly where such outputs may be relied upon for decisions affecting data subjects | "Ensure that appropriate safeguards, including verifiable content provenance and labelling mechanisms (e.g. metadata watermarking or equivalent disclosure techniques), are embedded and implemented to reduce the risk of hallucinations, inaccurate personal information, or misleading outputs concerning identifiable individuals, particularly where such outputs (synthetic audio, image or video content) may be relied upon for decisions affecting data subjects." | Generative AI models may be associated with frequent generations of false data, including biographical or credit details (hallucinations), which potentially undermine data accuracy contrary to the Data Protection Act (section 25) and the Constitution, especially Article 46 on consumer rights.<br><br>Similarly, it poses a threat to observance of the AfCFTA Protocol on Digital Trade, which is emphatic on consumer protection, building digital trust, and truthfulness in continental trade using automated electronic services. |

| | | | | |
|---|---|---|---|---|
| | | | | Labelling synthetic content is also consistent with the direction already taken in comparative international and regional practice. |
| 5. | Page 9, Section 3a<br>The Constitution of Kenya, 2010 | The constitutional basis only captures articles 31 (privacy), 27 (equality and non-discrimination), 46 (consumers' rights), 35 (access) | AI impacts the entire cross-section of human rights in the Bill of Rights, given its cross-cutting applications across society and its potential to promote or threaten realisation of all rights. Add Article 54 (rights of persons with disabilities to access information in accessible formats) to the effect "Article 54 guarantees the rights of persons with disabilities, including dignity and respect, access to educational institutions, reasonable access to information, use of sign language, and other appropriate means of communication and access to materials and devices to overcome constraints arising from the person's disability"<br><br>Address AI accessibility considerations in sections 4, 9 and annex 2. | AI is increasingly being deployed as assistive technology in areas such as text-to-speech and sign language recognition, but it can also exclude persons with disabilities when training data or biometric information are developed without them and for them. Addressing the persons with disabilities aspect will align the Guidance Note with the European Union (EU) AI Act, which sets a benchmark for how regulation can protect marginalised groups, and the AU Continental AI Strategy, which provides guiding principles on how AI should be developed, governed, and used across the continent. |
| 6. | Page 20, Section 7.6 (Children and AI Systems) | "Section 33 of the Act provides enhanced protections for children's personal data" | Cross-reference the Children Act 2022 (the best-interests principle and protection from online exploitation and abuse sections 22 (3) (c)) and section 2 (f) and the ODPC's own Guidance Note for Processing Children's Data (2025) as the primary reference | The ODPC already has a more detailed and dedicated guidance engaging with the Children Act (2022). There should be specific reference to the guidance note for consistency. It will also provide clarity to those using AI in education and child welfare (considered high-risk in Section 9 of the Guidance Note on the Processing of Children's Data) that more detailed guidance is available. |
| 7. | Pages 28-29 Table section | The high-risk table does not address AI use in the information ecosystem, especially in political and electoral contexts | Add a row on 'AI in Political Communication' covering risks such as voter micro-targeting based on inferred political views (which is considered sensitive personal data), electoral communication, and the use of AI-generated synthetic content in forms including audio, images, or videos of political players. Also include the requirement for a Data Protection Impact Assessment (DPIA), clearly | The AI Bill (2026) addresses issues such as deepfakes and AI-generated political content, and since explicit political opinion is referred to as sensitive personal data, it is critical that the office addresses this as it lies within the ODPC's mandate. |

| | | | | |
|---|---|---|---|---|
| | | | labeling AI-generated political content and working with the Communications Authority and IEBC. | |
| 8. | Page 33 Annex 1 (Registration row) | "Register as a data controller or processor with the ODPC at www.odpc.go.ke before deploying any AI system that processes personal data." | Add a note that once the AI Bill 2026 is enacted, entities operating high-risk AI systems should mandatorily register on the high-risk AI systems register maintained by the office of the AI Commissioner and clearly elaborate the partnership or independent working plan between the two entities. | The AI Bill 2026, as currently drafted, contains its own Commissioner-maintained public register of high-risk AI systems. Other entities that have a similar requirement may not be aware that this checklist is mandatory. Flagging this early avoids future shortcomings. |
| 9. | Page 30, Section 11 (AI Governance Framework) | Requires entities to establish algorithmic audit standards, but frames "AI systems" primarily around bespoke enterprise deployments (credit scoring, health diagnostics, fraud detection, etc.). | Clarify explicitly that algorithmic auditing and governance obligations extend to AI-powered recommender and content-curation systems (news feeds, "for you" pages, autoplay and recommendation engines) operated by digital platforms that process the personal data of persons in Kenya, regardless of whether the platform has a registered local entity. | CIPESA's research shows that the most pervasive form of AI Kenyans interact with is not enterprise chatbots but algorithmic feeds used by the country's 18.4 million social media users, and that most users do not recognise these systems as "AI" at all.[1] An AI governance framework that cannot reach the algorithmic curation layer of major platforms has, in practice, exempted the largest category of AI processing affecting Kenyans from meaningful oversight. |
| 10. | Pages 31–32, Section 13 (Enforcement and Complaints) | Describes the Office's general enforcement powers (investigations, audits, penalty notices, administrative fines) without addressing enforcement against AI providers that have no registered presence in Kenya. | Recommend that foreign AI providers, foundation model providers, and digital platforms that process personal data of persons in Kenya at scale, but have no registered local entity, designate a local representative or point of contact for data-subject-rights requests, complaints, and enforcement correspondence, modelled on comparable representative requirements in other data protection regimes. | A recurring theme in CIPESA's work on platform accountability in Africa is that dominant foreign technology companies frequently engage inconsistently, or not at all, with African regulators and civil society, leaving governments to negotiate individually and from a position of limited leverage.[2] A named local representative is a low-cost, high-value mechanism to make enforcement and redress practically accessible rather than merely theoretical. |
| 11. | Pages 7–8, Section 2.1 | Frames AI adoption in Kenya | Broaden the framing to acknowledge explicitly that | Kenya has been reported to have among the |

[1] *State of Internet Freedom in Africa 2025: Navigating the Implications of AI on Digital Democracy in Africa.* https://cipesa.org/wp-content/files/reports/State_of_Internet_Freedom_in_Africa_Report_.pdf

[2] Democratising big tech: Lessons from South Africa's 2024 election. https://cipesa.org/2025/07/democratising-big-tech-lessons-from-south-africas-2024-election/; Civil society and the fight for big tech accountability in Africa. https://cipesa.org/2026/08/civil-society-and-the-fight-for-big-tech-accountability-in-africa/

| | | | | |
|---|---|---|---|---|
| | (Background) | primarily around enterprise and government use cases (credit scoring, diagnostics, predictive policing, employment screening, personalised advertising, benefits administration). | the dominant, most pervasive form of AI processing personal data of persons in Kenya today is embedded in foreign-owned consumer platforms and generative AI tools consumed by, rather than built in, Kenya, and that this asymmetry (data and compute ownership offshore, data subjects and, increasingly, data-labelling labour onshore) is itself a distinct data protection and human rights concern. | highest rates of AI tool usage globally, but this measures consumption of AI built elsewhere, not domestic AI capability; the same systems are frequently trained in part on data annotation and content moderation labour performed by Kenyan workers under difficult conditions.[3] The omission leaves the larger, offshore-controlled AI largely unaddressed. |
| 12. | Section 7 (Obligations of Data Controllers and Data Processors), generally | The obligations set out (registration, DPIA, DPO, breach notification, third-party processor agreements) are framed around the personal data of the AI system's end users and data subjects. | Add a clause requiring entities that train or fine-tune AI models using human data annotators, content moderators, or reinforcement learning from human feedback (RLHF) workers located in Kenya to extend equivalent data protection safeguards to the personal data of that workforce, including in any associated monitoring, performance-scoring, or psychological-support data processing. | CIPESA's analysis of Kenya's AI ecosystem highlights that data annotators and content moderators in Nairobi's outsourcing centres, who absorbed some of the most harmful training-data review work for major foreign AI labs at low pay, are part of the personal data processing chain but are largely invisible in current AI governance discourse.[4]<br><br>The Guidance Note should genuinely aim at protecting the "whole of society" and extend its data protection lens to this workforce, not only to the eventual end users of the resulting AI systems. |
| 13. | Page 28–29, Section 9 (High-Risk Table, Row: AI in Law Enforcement and Public Safety) | "Specific statutory authority required; DPIA mandatory; independent oversight; restrictions on automated profiling for law enforcement purposes." | Add: "...; prohibition on indiscriminate or generalised AI-enabled biometric surveillance of the population; prior judicial or independent authorisation required for any targeted, AI-assisted biometric surveillance; mandatory linkage assessment where the AI system draws on, or feeds into, national identity or biometric registries (e.g., Maisha Namba), with DPIA renewal triggered whenever a registry-linked AI use case changes." | National security and public administration use of AI is treated only glancingly. The Guidance Note does not address predictive policing, AI-enabled biometric surveillance by security agencies, or the accountability failures.<br><br>Kenya's High Court has twice halted government biometric ID rollouts for inadequate safeguards and absent DPIAs. Yet the database (Maisha Namba/IPRS) now underpins numerous |

[3] Kenya doesn't have an AI regulation gap, it has an accountability gap. https://cipesa.org/2026/05/kenya-doesnt-have-an-ai-regulation-gap-it-has-an-accountability-gap/

[4] *Kenya doesn't have an AI regulation gap, it has an accountability gap.* https://cipesa.org/2026/05/kenya-doesnt-have-an-ai-regulation-gap-it-has-an-accountability-gap/

| | | | | |
|---|---|---|---|---|
| | | | | downstream AI-adjacent uses, reportedly accessible to over 450 entities. International standards require AI-enabled surveillance to be lawful, necessary, proportionate, non-discriminatory, and independently overseen.<br><br>The Guidance Note should be revised to explicitly capture AI systems built on top of, or fed by, national identity and biometric registries, and to require the same DPIA and independent-oversight standard applied to Huduma Namba and Maisha Namba by the courts.<br><br>The Guidance Note should also acknowledge the institutional tension between the security agencies most likely to deploy AI-enabled surveillance and the constitutional and statutory limits on such deployment. Under international human rights law, AI-enabled mass surveillance is incompatible with human rights law, and any targeted use must be authorised by law, necessary and proportionate to a legitimate aim, non-discriminatory, and subject to independent oversight and judicial safeguards.<br><br>Public administration deserves separate treatment from law enforcement because the harms are different in kind: they are distributive and administrative rather than punitive, but they can still be severe, opaque, and difficult to contest. |
| 14. | New sub-section proposed after Section 7.9 (renumber as Section 7.10: AI Systems Built on Digital Public Infrastructure) | No equivalent provision exists. The Guidance Note does not address AI systems layered onto shared government data infrastructure (digital ID, health financing, tax systems). | Add Section 7.10 requiring: (i) a whole-of-government DPIA before any new AI-enabled use case is added to an existing DPI platform; (ii) publication of data-sharing agreements and legal basis governing inter-agency data flows feeding the AI system; (iii) mandatory algorithmic-transparency | Kenya is one of the more advanced African states in building Digital Public Infrastructure (DPI): interoperable digital identity (Maisha Namba), a unified digital payments ecosystem, and increasingly integrated government data platforms feeding services, and is now |

| | | | | |
|---|---|---|---|---|
| | | | disclosure, including publication of scoring methodology or formula, subject to narrowly drawn security exceptions; and (iv) a standing requirement that DPI-linked AI systems affecting eligibility for public services provide affected persons a right to a documented, reasoned explanation and human review. | integrating AI-driven decision-making and eligibility scoring.<br><br>The risks of DPI are different from enterprise systems largely because DPI systems are typically mandatory and effectively non-optional for accessing essential services, which forecloses consent as a meaningful lawful basis and places the entire weight of protection on the public-interest/official-authority basis. Second, DPI systems are increasingly interoperable by design, meaning data collected for one purpose becomes an input into AI-driven eligibility or scoring systems for a different purpose, raising acute purpose-limitation concerns. Third, DPI is often built and hosted in partnership with local and foreign technology vendors and cloud providers, inheriting the cross-border and big-tech accountability risks, with the added complication that the data controller is the state or a state institution.<br><br>The SHA case study shows what happens without such safeguards: an undisclosed methodology overcharged the poorest households, with no meaningful avenue for a household to understand or contest its assessment.[5] |
| 15. | Page 8, Section 2.2 (Privacy and Data Protection Concerns in AI) | Lists opacity, bias, excessive collection, re-identification, cross-border flows, children/vulnerable groups, generative AI risks, inferred data, | Add a new concern: "Repurposing for national security and surveillance: personal data and biometric datasets collected for commercial, administrative, or welfare purposes may be repurposed for state security, surveillance, or | Surveillance capitalism and the militarisation of AI are presenting new risks with the convergence of commercial behavioural profiling with state security and military AI use. International bodies warn that civilian |

[5] The Guardian. (2026, May 4). Flaws in Kenya's AI-driven healthcare reforms driving up costs for the poorest. https://www.theguardian.com/global-development/2026/may/04/kenya-ai-healthcare-reforms-driving-up-costs-for-poor; Office of the United Nations High Commissioner for Human Rights (OHCHR). (2025, October). Protecting human rights while using artificial intelligence in counter-terrorism: Position paper and recommendations of the UN Special Rapporteur on Counter-Terrorism. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/activities/2025-10-un-sr-ct-recommendations-ai-position.pdf

| | | | | |
|---|---|---|---|---|
| | | and "emerging AI risks (bias, drift, and security)" without naming repurposing of data for security/surveillance/military use. | military-adjacent uses without data subjects' knowledge or a fresh legal basis.<br><br>Such repurposing shall require an independent, documented, and judicially reviewable determination of necessity, proportionality, and legal basis before it may occur." | AI/biometric infrastructure lowers the threshold for security and military repurposing.[6] The commercial logic of surveillance capitalism, in which personal data is captured and exploited at a scale individual consent cannot govern, converges with, and increasingly normalises, state surveillance, which uses the same data and infrastructure.<br><br>The OHCHR cautions that AI-enabled surveillance and biometric tools already deployed in civilian contexts create the technical infrastructure that lowers the threshold for subsequent security and military repurposing. Thus, the risk is that biometric and AI systems built for civilian administrative purposes create data assets that can be repurposed for surveillance without the original data subjects' knowledge or a fresh legal basis. |
| 16. | Page 13–14, Section 4.6 (Integrity and Confidentiality) and Page 25, Section 8.3 (Model Training and Development) | Refers to "model inversion or membership inference attacks capable of reconstructing training data" and requires "appropriate technical and organisational security measures for training infrastructure," without a systematic AI-cybersecurity framework. | Add a dedicated sub-clause requiring entities to: (i) maintain documented data lineage and integrity controls to detect data poisoning in training pipelines; (ii) conduct periodic adversarial-robustness testing for high-risk AI systems, particularly biometric and fraud-detection systems; (iii) test deployed models for susceptibility to membership-inference and model-inversion attacks before relying on anonymisation as a safeguard; (iv) implement controls against model extraction/theft via repeated-query attacks on deployed inference APIs; and (v) adopt an internal policy governing employee use of third-party generative AI tools | Current security research identifies at least five categories of attack that specifically target the personal data embedded in AI systems: (i) data poisoning; (ii) adversarial examples; (iii) model inversion and membership inference; (iv) model extraction or theft; and (v) prompt injection and "shadow AI" risk from unsanctioned employee use of generative tools.[7]<br><br>As government AI expands into DPI systems handling identity, health, and tax data, the attack surface affecting millions of Kenyans' personal data grows correspondingly. |

[6] Office of the United Nations High Commissioner for Human Rights (OHCHR). Briefer on human rights and artificial intelligence in the military domain. https://www.ohchr.org/en/documents/brochures-and-leaflets/briefer-human-rights-and-artificial-intelligence-military-domain

[7] Radware. (2025, December 17). AI security in 2026: Threats, core principles and defenses. https://www.radware.com/cyberpedia/ai-security/; SentinelOne. (2024, October 29). Top 14 AI security risks in 2026. https://www.sentinelone.com/cybersecurity-101/data-and-ai/ai-security-risks/; Suzu Labs. (2026, July 10). Top 7 AI security risks in 2026. https://suzulabs.com/suzu-labs-blog/top-7-ai-security-risks-in-2026

| | | | | |
|---|---|---|---|---|
| | | | ("shadow AI") to prevent uncontrolled transfer of personal data outside approved data processing agreements. | |
| 17. | Page 28–29, Section 9 (High-Risk Table) — new row proposed | No row addresses AI-driven eligibility scoring or means-testing for public benefits or social protection. | Add a row: "AI/Algorithmic Means-Testing and Benefits Eligibility Scoring (e.g., health-insurance premium determination, social-protection targeting)" — Primary Risks: opaque scoring formulae; disparate impact on low-income households; absence of contestability — Specific<br><br>Obligations: DPIA mandatory before deployment and before any material change to the scoring model; publication of the scoring methodology and the categories of indicators used; mandatory, accessible human review mechanism under Section 35; independent, pre-deployment equity testing of the model's distributional impact across income groups, with results published. | An Africa Uncensored/Lighthouse Reports/Guardian investigation (May 2026) found that the Social Health Authority's AI-driven proxy-means-testing model, which sets household health-insurance premiums using indicators such as roofing material and toilet type, systematically overcharged the poorest households while undercharging wealthier ones.[8] The published account of the methodology referred only broadly to "household-specific and individual-specific indicators" without disclosing the underlying formula or weighting, leaving affected households unable to understand, contest, or seek meaningful human review of their premium determination.<br><br>A consultancy (ID Insight) had warned before launch that the model was "highly likely to miscalculate contributions for low-income households"; that warning was not acted on. The published methodology description did not disclose the underlying formula or weighting, leaving affected households unable to contest their assessment — a direct violation of the transparency and automated-decision-making principles in Sections 6.1 and 6.6 of the Guidance Note. |
| 18. | Page 28–29, Section 9 (High-Risk Table) — new | No row addresses AI-assisted tax administration or compliance | Add a row: "AI-Assisted Tax Compliance Validation and Cross-Referencing (e.g., automated income tax | From January 2026, KRA began automated, systematic validation of income tax returns |

[8] The Elephant. (2026, May 6). Hiding behind AI: How SHA was used to load health system costs onto poorest. https://www.theelephant.info/investigations/2026/05/06/hiding-behind-ai-how-sha-was-used-to-load-health-system-costs-onto-poorest/; The Guardian. (2026, May 4). Flaws in Kenya's AI-driven healthcare reforms driving up costs for the poorest. https://www.theguardian.com/global-development/2026/may/04/kenya-ai-healthcare-reforms-driving-up-costs-for-poor

| | | | | |
|---|---|---|---|---|
| | row proposed | validation. | return validation against eTIMS, withholding, and customs data)" — Primary Risks: large-scale data-matching across multiple state and private data sources; automated flagging with direct financial consequences; limited taxpayer visibility into flagging logic — Specific Obligations: DPIA mandatory; documented right to request human review of automated compliance flags under Section 35; clear, accessible explanation mechanism for flagged taxpayers; data-minimisation review of cross-referenced datasets. | against eTIMS electronic invoicing, withholding-tax, and customs import data, describing this as a shift to "data-driven income and expense validation".[9]<br><br>This is functionally equivalent to the AI credit-scoring and fraud-detection use cases the Guidance Note already treats as high-risk when performed by private lenders, and should be held to the same standard when performed by a state revenue authority. |
| 19. | Page 31, Section 13 (Enforcement and Complaints) — closing paragraph | Lists categories of complaints (failure to disclose AI processing, absence of human review, discriminatory profiling, etc.) without an explicit category for government/DPI-linked AI systems or national-security-related processing. | Add to the illustrative list of complaint categories: "unlawful repurposing of personal data collected for administrative, welfare, or commercial purposes for national-security, surveillance, or military-adjacent use without independent authorisation; and opaque or non-contestable AI-driven eligibility, means-testing, or tax-compliance determinations by public bodies."<br><br>Add a corresponding commitment that the Office will accept and adjudicate complaints against public bodies, including security agencies, on the same footing as private entities. | Without an explicit statement that public bodies, including security and revenue agencies, are subject to the same complaints and enforcement regime as private entities, data subjects and civil society may reasonably doubt whether the Office's enforcement powers extend in practice to the government's own highest-risk AI deployments, which are, on the evidence reviewed in this submission, currently among the least transparent.[10] |

[9] KPMG Kenya. (2026, January). eTIMS and the shift to data-driven income and expense validation. https://kpmg.com/ke/en/insights/2026/01/eTIMS-and-the-shift-to-data-driven-income-and-expense-validation.html; CIO Africa. (2025, November 10). KRA to begin automated validation of tax returns. https://cioafrica.co/kra-to-begin-automated-validation-of-tax-returns/

[10] The Guardian. (2026, May 4). Flaws in Kenya's AI-driven healthcare reforms driving up costs for the poorest. https://www.theguardian.com/global-development/2026/may/04/kenya-ai-healthcare-reforms-driving-up-costs-for-poor