# CIPESA Submission on the Draft Guidance Note on Emerging Technologies

**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**Name of the Guidance Note: Draft Guidance Note on Emerging Technologies**

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**RE: SUBMISSION ON THE DRAFT GUIDANCE NOTES ON EMERGING TECHNOLOGIES**

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). Our comments focus on areas where CIPESA's work on digital rights, AI governance and data governance in Africa offers specific recommendations, rather than providing a comprehensive line-by-line review.

CIPESA recommends that the Guidance adopt a risk-based, rights-respecting and innovation-enabling approach. As guidance under Kenya's data protection framework, it should provide clear and practical direction on applying existing data protection obligations to emerging technologies, while avoiding blanket restrictions that are not justified by the nature, context, or severity of the risks involved.

The Guidance should be interpreted consistently with the Constitution, the Data Protection Act, the Malabo Convention, the AU Data Policy Framework, the AU Continental AI Strategy and the AfCFTA Protocol on Digital Trade. These frameworks support the protection of privacy, equality and other fundamental rights while enabling responsible innovation, data-driven development, and legitimate cross-border digital activity. In particular, the AU Data Policy Framework promotes people-centred data governance and responsible data use, while the AU Continental AI Strategy advances an Africa-centric, development-oriented and inclusive approach to AI. CIPESA therefore recommends proportionate safeguards for higher-risk emerging technologies, without creating unnecessary barriers to innovation and legitimate cross-border digital activity.

Yours sincerely,

CIPESA Team

| No. | Page No. & Section of Guidance Note | Statement as currently captured | Proposed Statement | Comments/Justification |
|---|---|---|---|---|
| 1. | Page 13-14, Paragraph 6 on Cloud Computing | ***Page 14 para 1 section 6.1:*** "The Office notes that data localisation considerations may arise in specific contexts, including for data relating to the strategic interests of the state. Entities processing personal data in connection with critical national infrastructure, national security, or strategic government functions should assess whether applicable law or policy imposes data localisation requirements that may constrain cloud deployment options." | Data localisation, including requirements on the location of computing facilities, shall not be a general condition for cloud deployment, except where a specific statutory localisation requirement applies. Any other localisation requirement shall be grounded in clear and accessible law, pursue a legitimate public policy or essential security objective, and be applied without discrimination | Article 22(1) of the AfCFTA Protocol on Digital Trade bars conditioning digital trade on the location of computing facilities, while Article 22(2) permits exceptions only where necessary to achieve a legitimate public policy or security objective, applied without discrimination and no more restrictively than necessary. The reference to "strategic interests of the state" risks becoming a de facto localisation rule without these safeguards. Specific statutory localisation requirements, including those under Section 50 of the Act and Regulation 26 and reflected in the ODPC's Guidance Note on Biometric Data, would continue to apply. This is also consistent with the AU Data Policy Framework's emphasis on responsible intra-African data flows. |
| 2. | Pages 16-17, Section 8.4-8.5 and pages 26-27, section 13.8<br><br>"Surveillance/mass identification (N: N or open-set N:1)" and "Data Protection Concerns in Biometric Recognition Systems" | Sec.8.4 "Surveillance biometrics is the highest-risk mode, raises the most concerns under the Act and the Constitution, and is treated as such in the obligations below."<br><br>Page 26, last para; "…data handlers should ensure that such deployments satisfy the requirements of the Data Protection Act and are | Amend **Secs 8.4 and 13.8** to read:<br>Real-time remote biometric identification and mass biometric surveillance in publicly-assessible spaces by r public or private entities shall not be permitted for indiscriminate or generalised surveillance. Biometric categorisation to infer sensitive characteristics and AI-based emotion recognition in education and employment settings shall not be permitted. Remote biometric identification for law enforcement purposes shall only be permitted only where expressly authorised by law, strictly necessary | Surveillance biometrics at scale raises serious privacy and equality concerns under Article 31 and Article 27 of the Kenyan Constitution.<br><br>Article 14 of the Malabo Convention supports heightened protection for sensitive data of this kind; while Article 5(1)(h) of the EU AI Act provides a useful comparison as it bars biometric identification and emotion recognition in school and workplaces, and stipulates the narrow conditions applicable to real-time remote biometric identification for law enforcement. |

| | | | | |
|---|---|---|---|---|
| | | demonstrably necessary and proportionate, and comply with the specific safeguards contained in the ODPC's Guidance Note on Biometric Data" | and proportionate to a specific objective, limited in scope, duration and geography, subject to judicial warrant and oversight. | The ODPC's Guidance Note on Biometric Data identifies "surveillance and tracking" as a privacy concern but does not provide a specific safeguard or authorisation requirement. The proposed text therefore clarifies the safeguards applicable for these high-risk uses and is consistent with the AU Continental Artificial Intelligence Strategy's human rights approach. |
| 3. | (Pages 23–24) Section 13.3 Data Protection Impact Assessment | "A DPIA is required before deploying any emerging technology system that is likely to result in high risk to the rights and freedoms of data subjects. Processing of personal data using new technologies is considered high-risk processing. Accordingly, all emerging technology deployments that involve the processing of personal data are subject to a DPIA. Such deployments include.." | "A DPIA is required before deploying any emerging technology system that is likely to result in high risk to the rights and freedoms of data subjects. An Executive Summary of the assessment, withholding only intellectual property, proprietary trade, and trade secrets details, shall be published on the ODPC Public High-Risk Technology Register before deployment." | Publication of standardised DPIA summaries will foster transparency and accountability and build public trust in high-risk emerging technology deployments.<br><br>This will also align the provisions with Article 31 of the Kenyan Constitution on privacy, the transparency directives of the AU Continental Artificial Intelligence Strategy, and Article 27 of the EU AI Act Article 27 which provides for the publication of the fundamental rights impact assessment. |
| 4 | Pages 22, Section 12.6 "Right Not to Be Subject to Automated Decision-Making"; Page 24, Section 13.7 "General Obligations for Emerging Technology Deployments" | "Entities shall implement human review mechanisms, provide explanations of automated decisions upon request, and enable data subjects to contest automated outcomes." | Where an emerging technology system makes or materially informs a decision that has legal or similarly significant effects, the controller shall provide meaningful information about the principal factors and data relied upon in reaching the decision; provide human review by a person with actual authority to overturn or modify the outcome; enable the affected person to contest the decision and seek correction of inaccurate data; and maintain records of system performance and human interventions. These safeguards shall apply particularly where decisions affect employment, credit, insurance, education, healthcare, social protection, | A right to human review is of limited value if the reviewer simply rubber-stamps an automated output. Requiring actual authority to overturn or modify the outcome makes review meaningful. Providing information about the principal factors and data relied upon gives data subjects a basis to contest a decision without requiring disclosure of source code or proprietary algorithms. This approach is also consistent with the AU Continental AI Strategy's emphasis on meaningful recourse and human oversight over consequential automated decisions. |

| | | | | |
|---|---|---|---|---|
| | | | immigration, policing or access to public services, including where children or other persons at heightened risk are affected. | |
| 5. | Pages 9–10, Section 3 "Legislative Framework"; Pages 13–14, Section 6.1 "Data Protection Concerns in Cloud Computing" | Limited framework governing national security or law enforcement access to data processed through emerging technology. | Access to personal data held or processed through emerging technology systems for national security or law enforcement purposes shall be grounded in clear law and be necessary and proportionate to a specific objective. Intrusive surveillance shall require prior judicial or independent authorisation. Controllers and processors shall maintain appropriate records of requests and disclosures. Public authorities shall, where legally permissible, publish aggregate information on government access requests, without disclosing the existence or details of active covert investigations. National security shall not, by itself, exempt a deployment from applicable data protection safeguards. | National security should not operate as a blanket exemption from applicable data protection safeguards. This complements Row 2 by establishing broader expectations for lawful access, transparency and accountability beyond biometric surveillance. The recommendation is grounded in Articles 31 and 27 of the Constitution and does not displace statutory requirements governing protected or confidential information. |
| 6. | Pages 23-24, Section 13.1 "Registration" and Section 13.3 "Data Protection Impact Assessment" | Registration and DPIA requirements apply uniformly regardless of deployment scale | The Office should provide simplified registration and DPIA templates for SMEs, research institutions and civil society organisations undertaking low-risk or limited-scale deployments, without reducing substantive protections. For genuinely novel or uncertain use cases, the Office should consider establishing supervised regulatory sandbox arrangements with defined scope, safeguards, monitoring and exit criteria. | These are institutional and operational recommendations rather than proposed textual amendments. Simplified compliance would reduce unnecessary burdens for known low-risk actors, while sandboxing would help manage regulatory uncertainty for genuinely novel deployments. A small civil society pilot should not carry the same procedural burden as a national biometric rollout. Article 23 of the AfCFTA Protocol on Digital Trade recognises regulatory sandboxes for data innovation. |

**About CIPESA**

The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) works to defend and expand the digital civic space to enable the protection and promotion of human rights and to enhance innovation and sustainable development. With a focus on disparate actors including the private sector, civil society, media, policymakers, and multinational institutions, our work aims to engender a free, open, and secure internet that advances rights, livelihoods, and democratic governance.

CIPESA's work responds to a shortage of information, research, resources, and actors consistently working at the nexus of technology, human rights, and society. Indeed, CIPESA's establishment in 2004 was in response to the findings of the Louder Voices Report for DFiD, which cited the lack of easy, affordable, and timely access to information about ICT-related issues and processes as key barriers to effective and inclusive ICT policy-making in Africa.