

PUBLIC CONSULTATION / REGULATORY ENGAGEMENT

Comments on Draft Guidance Note on Emerging Technologies

Submitted by the African Centre for AI Governance and Oversight (ACAIGO)

SUBMITTED TO	Office of the Data Protection Commissioner
OUR REF:	ACAIGO/SE/2/2026
DATE	17 th August 2026
CONTACT	Email: info@acaigo.africa , website: https://www.acaigo.africa/

Executive summary

ACAIGO welcomes the opportunity to provide comments on the Draft Guidance Note on Emerging Technologies. Our comments consider the clarity, legal consistency and practical application of the proposed guidance, with a view to supporting guidance that effectively addresses the processing of personal data in the context of emerging technologies while remaining consistent with Kenya's data protection framework.

KEY RECOMMENDATIONS

- Align the Guidance Note with the Data Protection Act
- Strengthen the guidance on cross-border transfers of personal data
- Refine the examples used in the Guidance Note

Detailed comments

Page No.	Statement as currently captured	Proposed Statement	Comments/Justification
11	Entities shall establish and enforce data retention policies that specify the maximum period for which personal data generated by each emerging technology will be retained.	Entities shall establish and enforce data retention policies that specify the maximum period for which personal data processed through each emerging technology will be retained.	The provision focuses on personal data generated by emerging technologies. This may be interpreted to exclude personal data collected, obtained, uploaded, stored or otherwise processed through those technologies. The retention obligation should apply to all personal data processed through an emerging technology, including input data and data inferred, derived or generated by the system.
13,14	Example Afya Digital shall: Afya Digital, a private hospital chain, migrates its patient records management system to a cloud-based SaaS platform operated by an international provider whose servers are located in the European Union and the United States. • enter into a data	Afya Digital, a private hospital chain, migrates its patient records management system to a cloud-based SaaS platform operated by an international provider whose servers are located in the European Union and the United States. Afya Digital shall:	The example should distinguish between adequacy and an assessment of appropriate safeguards. Under regulation 44 of the Data Protection (General) Regulations 2021, determining whether a country, territory, specified sector or international organisation ensures an adequate level of

processing agreement with the SaaS provider; • assess the adequacy of data protection in the EU (likely adequate) and the US (requires additional safeguards);	• enter into a data processing agreement with the SaaS provider; • assess and document the existence of appropriate safeguards for transfers to both the European Union and the United States; • implement appropriate contractual, technical and organisational safeguards for transfers to both jurisdictions; • conduct a DPIA, given the sensitivity of health data and the scale of processing; • ensure that the DPO is involved in the migration decision; and verify that the SaaS provider and its sub-processors do not process personal data in any jurisdiction without appropriate safeguards	protection is the responsibility of the Data Commissioner. Afya Digital may not independently determine that the European Union is “likely adequate.” Moreover, the ODPC has not, to date, issued an adequacy decision recognising the European Union as providing an adequate level of protection under Kenyan law. In the absence of an applicable adequacy decision, Afya Digital should assess and document whether appropriate safeguards exist under regulation 41 and implement the necessary contractual, technical and organisational measures for transfers to both jurisdictions. The current wording is therefore not merely imprecise; it misallocates statutory authority and risks encouraging controllers and processors to make informal adequacy determinations that the Regulations reserve for the Data Commissioner. Regulations 40, 41 and 44 support this distinction.
---	---	--

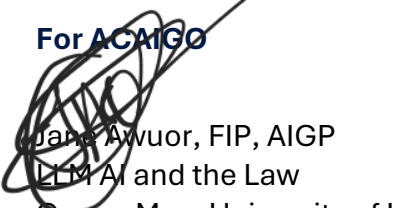
18	Example EduVR, a Nairobi-based edtech company, deploys a VR platform for secondary school students that tracks students' gaze patterns, movement, and engagement levels during virtual lessons. The company shall: • recognize that gaze tracking data constitutes biometric data (sensitive personal data); • establish explicit consent from parents or guardians, given the students are minors as the lawful basis; • conduct a DPIA; • provide parents and students with a privacy notice in plain, age-appropriate language; • implement data minimization, collecting engagement metrics rather than raw biometric data where the educational purpose can be served; and • prohibit any use of the biometric data for commercial profiling.	ACAIGO refrains from proposing a revised example and invites the Office to reconsider the example considering the concerns identified above.	The example appears to presume that the collection of children's gaze patterns, movements and engagement levels is permissible provided that parental consent and specified safeguards are implemented. This framing is problematic because parental consent does not, by itself, render intrusive monitoring of children necessary, proportionate or consistent with their best interests. Section 33 of the Data Protection Act requires the processing of children's personal data not only to be supported by parental or guardian consent but also to be conducted in a manner that protects and advances the child's rights and best interests. The schools should therefore be required, as a preliminary matter, to demonstrate that the monitoring is strictly necessary for a clearly defined educational purpose and that the same purpose cannot reasonably be achieved through less intrusive means. The example should also address whether consent can be freely
----	---	---	--

			withheld without excluding or disadvantaging a student and should prohibit the use of the data for behavioral, disciplinary or other consequential profiling, rather than limiting the prohibition to commercial profiling. As presently framed, the example risks normalizing continuous biometric or behavioral surveillance of children merely because procedural safeguards have been adopted. Additionally, the example, as presently framed, does not clearly distinguish the roles and responsibilities of EduVR and the school with respect to data protection compliance,
24	Entities whose core activities involve large-scale systematic monitoring of data subjects through emerging technology systems, including IoT monitoring platforms, biometric recognition systems, connected vehicle fleet operators, and smart city infrastructure operators or large-	Entities whose core activities involve large-scale systematic monitoring of data subjects through emerging technology systems, including IoT monitoring platforms, biometric recognition systems, connected vehicle fleet operations and smart-city infrastructure, or the large-scale processing	Section 24(1) of the Data Protection Act provides that a data controller or data processor may designate or appoint a DPO in the circumstances specified under that provision. The use of “may” confers discretion and does not establish a mandatory obligation to appoint a DPO. By

	scale processing of sensitive personal data through such systems, shall designate a DPO under Section 24 of the Act. The DPO shall be involved in all DPIA processes, technology procurement decisions, and data subject rights responses relating to emerging technology systems.	of sensitive personal data through such systems, should consider designating or appointing a DPO under section 24 of the Act. Given the nature, scale and risks associated with such processing, the designation or appointment of a DPO is strongly advisable. Where a DPO has been designated or appointed, the DPO should be involved, in a timely manner, in DPIA processes, technology procurement decisions and responses to data-subject rights requests relating to emerging technology system	stating that the relevant entities “shall” designate a DPO, the draft guidance converts a discretionary statutory provision into a binding requirement. Although appointing a DPO may constitute good practice and may be strongly advisable where an entity undertakes large-scale systematic monitoring or processes sensitive personal data on a large scale a guidance note cannot create an obligation that is not imposed by the enabling legislation. The wording should therefore be revised to preserve the discretionary language of section 24 while emphasizing the heightened importance of DPO oversight in these circumstances.
29	Register with the ODPC as a data controller or processor before deploying any emerging technology system that processes personal data of persons in Kenya.	Determine whether the entity is required to register as a data controller or data processor under section 18 of the Act and the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021. Where registration is required, register with the ODPC before	The current statement implies that every entity deploying an emerging technology system that processes the personal data of persons in Kenya must register with the ODPC. However, regulation 13(2) of the Data Protection (Registration of Data Controllers and Data Processors)

		commencing the processing of personal data through an emerging technology system.	Regulations 2021 provides an exemption from mandatory registration based on an entity's annual turnover or revenue and number of employees. Although the scope of that exemption is subject to the other provisions of regulation 13, the checklist should not present registration as an unqualified obligation applicable to every entity. It should instead require entities to determine whether they are subject to mandatory registration under section 18 of the Act and the Registration Regulations.
--	--	---	---

For ACAIGO


Jane Awuor, FIP, AIGP
LLM AI and the Law
Queen Mary University of London

AFRICAN CENTRE FOR AI GOVERNANCE AND OVERSIGHT

<https://www.acaigo.africa/> | info@acaigo.africa | Nairobi, Kenya