ARTICLE 19 Eastern Africa

Memorandum

Public Consultation on the Draft Data Protection Regulations, 2021

To: The Ministry of Information, Communication, Technology, Innovation and Youth Affairs

Executive Summary

ARTICLE 19 Eastern Africa (or **ARTICLE 19 EA**) presents this memorandum in response to the draft Data Protection (General) Regulations, 2021 (or **draft Regulations**) currently being considered by the Ministry of Information, Communication, Technology (or **ICT**), Innovation and Youth Affairs.

ARTICLE 19 EA has analysed the draft Regulations for its compliance with international, regional and national privacy and data protection, freedom of expression (or **FOE**), and access to information (or **ATI**) standards. ARTICLE 19 EA notes that various provisions of the draft Regulations are positive and are consistent with relevant standards. Despite this, ARTICLE 19 EA is concerned that some provisions require amendments or deletion to ensure that the protections in the draft Regulations are in harmony with the fundamental rights to privacy, freedom of expression and the right to information as recognised under the Constitution of Kenya, 2010 (or **Constitution**) and in international law. The current draft fails to flesh out the provisions on the processing of personal data by the media which is inadequate to protect freedom of expression and does not contain provisions which promote consistency with the Access to Information Act 2016 and the Constitution.

Recommendations

1. We recommend:
    a. that the conditions for consent under Section 32 of the Data Protection Act 2019 (or **DPA 2019**) be read alongside the definition of consent provided under Section 2 of the DPA 2019. Specifically, prior to the processing of personal data, data controllers/processors must identify themselves to data subjects prior to the processing of personal data and must clearly identify the purpose or purposes of their proposed processing.
    b. that responses to data access requests by data controllers/processors be accompanied with a time limit to promote the right to access information under Article 35 of the Constitution.
    c. that the wide grounds permitting a data controller/processor to refuse to comply with a data access request be amended and aligned with the permissible limitations of the right to know under national, regional and international law.
    d. the deletion of the provision attempting to expand the national security exemption by focusing on national security *organs*, rather than properly-defined national security *purposes*.
    e. amendments to the draft Regulations and the DPA 2019 to ensure that the journalistic exemption provision is expanded beyond the principles of data protection, to canvass other crucial substantive and administrative provisions.

MATRIX PRESENTATION
THE DRAFT DATA PROTECTION (GENERAL) REGULATIONS, 2021

Draft Regulation	Provision	Proposal	Justification
Regulation 4	*Consent by data subject*	We recommend amendments to this provision	ARTICLE 19 EA notes that the conditions for consent under Section 32 of the Data Protection Act 2019 (or **DPA 2019**) must be read alongside the definition of consent provided under Section 2 of the DPA 2019. Under the DPA 2019, **"consent"** means any manifestation of ***express, unequivocal, free, specific and informed*** indication of the data subject's wishes by a statement or by a ***clear affirmative action***, signifying agreement to the processing of personal data relating to the data subject" (*emphasis added*). ARTICLE 19 EA notes that the draft Regulations are inconsistent with the definition of 'consent' under the DPA 2019 and international law and standards for the following reasons: a. The requirement for consent to be 'informed' is not satisfied under Regulation 4 (1), draft Regulations. Specifically, the four (4) requirements for consent under this draft regulation fail to i. oblige data controllers/processors to identify themselves to data subjects prior to the processing of personal data; and ii. oblige data controllers/processors to clearly identify the purpose or purposes of their proposed processing. b. The requirement for consent to be an 'express', 'unequivocal' and a 'specific'

			statement or a *clear affirmative action* is not promoted by the use of the language 'may' rather than '**shall**' or '**must**' prior to the processing of their personal data under Regulation 4 (4), draft Regulations. In effect, this renders the safeguards under Regulations 4 (5) and (6), draft Regulations moot, given the failure to expressly require data subjects to actually consent prior to their personal data being processed.
Regulation 8	*Data access request*	We recommend amendments to this provision and the addition of an appeal mechanism	The right to request access to personal data must be read concurrently with the right of access to information under Article 35 of the Constitution and the Access to Information Act (or **ATI Act**) 2016. ARTICLE 19 EA notes that Regulation 8, draft Regulations does not impose any time limit requirements on data controllers/processors to respond to data access requests, which risks interfering with data subjects' right to access their personal data and their right to know. ARTICLE 19 EA stresses that numerous jurisdictions impose a time limit during which a subject access request must be fulfilled by a data controller/processor. In the UK, controllers must respond to data access requests 'without undue delay but not later than **one (1) month** from the date of receipt of the request… whether it is a working day or not.' In Canada, privacy requests must be responded **within thirty (30) calendar days**. Analogously, the imposition of time limits for responses to information requests is firmly rooted under Section 9 (1), ATI Act 2016. Under this provision, public officers must respond to information requests **within twenty-one (21) days** of receiving the request, unless the information sought concerns the life or liberty of a person. ARTICLE 19 EA further notes that the grounds for refusal provided under Regulation 8 (4), draft Regulations are not aligned with the three-part test under

			international law and the permissible limitations of the right to access information under the Constitution. Additionally, the draft Regulations fail to provide an appeal mechanism for declined data access requests which risks interfering with the right to access justice under Article 48 of the Constitution. Despite Section 54 of the DPA 2019 permitting the Data Commissioner to 'prescribe other instances where compliance with certain provisions of this Act may be exempted', these exemptions must not 'limit the right or fundamental freedom so far as to derogate from its core or essential content.' In this instance, the terms 'public health' and 'public safety' have not been sufficiently defined in the draft Regulations, and may be used in a blanket manner to automatically reject subject access requests, thus interfering with the right to information. Notably, these grounds are not recognised as permissible limitations of the right to access information under Section 6 of the ATI Act 2016, which expounds on Article 35 of the Constitution. ARTICLE 19 EA notes that all data access requests must be considered by data controllers/processors, and we recommend the deletion of Regulation (4) (c), draft Regulations permitting a denial of a request on grounds that it is 'frivolous and vexatious.' This is not a permissible limitation of the right to information under the Constitution. The UK ICO clarified that the process of declining a request is not a 'simple tick list exercise' and that data controllers/processors must, *inter alia*, 'consider a request in the context in which it is made.'
Regulation 46	*Exemption for national security*	We recommend deletions and amendments to this provision	ARTICLE 19 EA emphasises that Regulation 46 (1), draft Regulations is misapplying the provisions of Kenya's Constitution by attempting to impose a blanket exemption on national security *organs*, rather than properly-defined national security *purposes*.

			Analogously, while Section 6 (1) (a) of the ATI Act 2016 provides that the disclosure of information may be limited where this is likely to 'undermine the national security of Kenya', the clarification provided under Section 6 (2) of the ATI Act 2016 makes reference to, and fleshes out, the *information* where this exemption may apply, rather than the organs themselves. Based on this, the purported expansion of the national security exemption not only introduces substantive amendments to the DPA 2019, but is also attempting to shift the parameters of Article 239 of the Constitution. These amendments exceed the mandate of the ICT Ministry and the Data Commissioner. We recommend that this specific reference to national security organs be deleted. Additionally, this proposed regulation fails to outline *specific purposes* where national security may constitute grounds for exemption, in a similar manner to Section 6 (2) of the ATI Act 2016. ARTICLE 19 EA stresses that a member of the Executive (i.e., the Cabinet Secretary) should not possess sole powers to determine what constitutes 'a processing for national security' without oversight from the judiciary. This exclusive power fails to comprehensively protect and promote the right to privacy and data protection, and also fails to satisfy the three-part test of legality, legitimacy, proportionality and necessity under international law.
General Comment			
General Comment	*Journalistic Exemption*	We recommend amendments to the draft Regulations and amendments to the Data Protection Act, 2019	ARTICLE 19 EA notes that the journalistic exemption provided under Section 52 of the DPA 2019 has not been expanded in the draft Regulations, with serious ramifications for the rights to freedom of expression and media freedom in Kenya. We recommend that this exemption be canvassed in the draft Regulations. This recommendation notwithstanding, the continued restriction of the journalistic

			exemption from the principles of processing personal data *only,* rather than other substantive and administrative provisions in the DPA 2019 raises serious consequences for the rights to freedom of expression and media freedom which must be addressed via amendments to the DPA 2019. By not being exempted from the registration requirements, journalists and the media will be obliged to inform the Data Commissioner about, among other things, the personal data being processed, for which purpose and the category of data subjects. Such an obligation poses serious risks for the confidentiality of journalistic sources and whistleblowers during investigations. Further, the journalistic exemption does not apply to the transborder data flow provisions under the DPA 2019 or the provisions in the draft Regulations. In effect, this means that journalists could be violating the provisions on transborder data flows when they publish any materials, including articles, audio, video, or images on the Internet or through other networks, and could be subject to civil and criminal penalties, even if the publication was legal in the originating country. **We call on the ICT Ministry to push for substantive amendments to the DPA 2019 to ensure that the mutually-reinforcing rights to privacy and data protection and freedom of expression and access to information are properly balanced.**

About ARTICLE 19 Eastern Africa

ARTICLE 19 Eastern Africa is a regional human rights organisation duly registered in 2007 as a non-governmental organisation in Kenya. It operates in fourteen (14) Eastern Africa countries and is affiliated to ARTICLE 19, a thirty (30) year old leading international NGO that advocates for freedom of expression collaboratively with over ninety (90) partners worldwide. ARTICLE 19 Eastern Africa leads advocacy processes on the continent with our sister organisations, ARTICLE 19 West Africa and ARTICLE 19 Middle East and North Africa.

Over the past 10 years, we have built a wealth of experience defending and promoting digital rights at the local, regional, and international levels. We have contributed to several Internet Freedom Policies, Data Protection, Cybercrime Bills and TV White Space Frameworks including Kenya's Draft Dynamic Spectrum Access Framework for Authorisation of the Use of TV White Spaces (2020), Kenya's Huduma Bill (2019), Kenya's Data Protection Bill(s) (2018/2019), Kenya's Cybercrime and Computer Related Crimes Bill 2014; Uganda's Data Protection and Privacy Act (2019), Uganda's Draft TV White Space Guidelines (2018); Tanzania's Cybercrime Act, 2015, among many others. We were also part of the Inter-Agency Technical Committee of the Ministry of ICT that developed the Kenya Cybercrime Bill, 2016 and the Kenya Data Protection Bill, 2018.

If you would like to discuss this analysis further, please email us at kenya@article19.org - with Mugambi Kiai (mugambikiai@article19.org) in copy - or call +254 727 862 230.