ARTICLE 19 Eastern Africa and Kenya ICT Action Network

Joint Memorandum

Public Participation on the Data Protection (Civil Registration) Regulations, 2020

To: Principal Secretary, State Department of ICT and Innovation

---

Executive Summary

ARTICLE 19 Eastern Africa (or **ARTICLE 19 EA**) and the Kenya ICT Action Network (or **KICTANet**) present this memorandum in response to the call for public participation on the said Data Protection (Civil Registration) Regulations, 2020 currently being considered by the Principal Secretary, State Department of Information Communication and Technologies (or **ICT**) and Innovation.

Recommendations

The following is a summary of our key recommendations:

1. The civil registration and identity management framework should be enacted through a stand-alone Act of Parliament. This should be subjected to (bicameral) legislative oversight and effective public participation. Notably, regulations should in practice provide general guidelines of practice, and cannot be used to regulate and create substantive systems which have implications on the effective and proper functioning of government, and which directly affect individuals' identity.
    a. **Recommendation:** Enact an 'appropriate and comprehensive' civil registration and identity management through an Act of Parliament introducing a Bill to amend the Registration of Persons Act (CAP 107).
2. The Data Protection Act (2019) cannot be used to give statutory effect to this civil registration system (or **CRS**) as that is not the objective of the Act. CRSs provide the 'foundation for national identity management systems'[1] and are inherently linked to the generation, collection and utilisation of vital statistics which inform a nation's development agenda, amongst other core functions. In Kenya, national identity management systems are provided for under the Registration of Persons Act (CAP 107) and the Citizenship and Immigration Act, 2011, the Refugees Act all of which legislate on CRS related issues, including national identity and the National Integrated Identity Management System (or **NIIMS**) in Kenya.

[1] UN (2019) 'Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management' <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwip2omK8O_nAhVE2-AKHTayDV8QFjADegQIBRAB&url=https%3A%2F%2Funstats.un.org%2Funsd%2Fdemographic-social%2FStandards-and-Methods%2Ffiles%2FHandbooks%2Fcrvs%2FCRVS_GOLF_Final_Draft-E.pdf&usg=AOvVaw0Vn4wgWRXQWjBEv-otbbD0>

a. **Recommendation:** Introduce a bill with these substantive amendments to the Registration of Persons Act which deals with civil registration, to address the inadequacies of the Act relating to civil registration. These regulations should not be anchored under the Data Protection Act, 2019.

3. The Regulations do not comply with the Data Protection Act (2019). In particular:

   a. Section 18 of the Data Protection Act (2019), requires the prior registration and certification of all data controllers collecting and processing copious amounts of sensitive personal data by the Data Commissioner. The provisions dealing with automated decision-making provide limited duties for data controllers and limit the rights of data subjects, in violation of the Data Protection Act (2019).

   b. Regulations 10 and 13 impose fees which are not stated and therefore could be a challenge for low income data subjects.

   c. The Regulations permit the retention of personal data by data controllers in perpetuity, despite the requirement for data to be retained in accordance with the 'reasonably necessary' requirement, and in any event, should provide the period of retention.

   d. The Regulations do not explicitly cater for, or have a mechanism to ensure that data breaches are notified to both the Data Commissioner, and data subjects, in line with section 43, Data Protection Act (2019) and international standards.

   e. The Regulations fail to provide for a mechanism capable of ensuring that the transfer of personal data through a public network is transmitted using strong encryption methods given the known weaknesses of commonly used encryption systems.

   f. The Regulations permit the transfer of personal data outside Kenya and directly contravenes sections 48 and 49 of the Data Protection Act (2019) as well as international standards.

   g. The Regulations fail to flesh out the 'adequacy' requirement.

   Recommendation: The government should fast-track the operationalisation of the Office of the Data Protection Commissioner (or **ODPC**) to ensure that there is proper oversight over the collection and processing of sensitive personal data in accordance

with the Data Protection Act (2019). The provisions of the proposed regulations should comply with the Data Protection Act, 2019.

4. The Regulations should provide explicit (*technical, personnel and procedural*) safeguards to ensure that personal information is accorded the highest safety and security, management and governance protection.

5. In conjunction with civil society and other stakeholders, the Ministry should develop 'appropriate and comprehensive regulatory frameworks' which adhere to the High Court's orders in Consolidated Petitions No. 56, 58 and 59 (2019) and which pay proper homage to the letter and the spirit of the Data Protection Act (2019) and international standards which Kenya is bound by.

General Comments: Matrix Presentation

General Comments		
Comment	**Proposal**	**Justification**
General Comment 1	We recommend amendments to the Registration of Persons Act (CAP 107)	The framework for civil registration should be provided through a stand-alone framework, which is subjected to legislative oversight and effective public participation. In 2019, the United Nations noted that civil registration systems affect the effective functioning of government, impact 'vital statistics and national identity management systems.'[2] Clearly, civil registration provisions should be effected via amendments to the Registration of Persons Act (CAP 107) and not the Data Protection Act (2019.
General Comment 2	We recommend amendments to ensure compliance with the Data Protection Act, 2019.	The data being collected by public organs, including biometric data, is sensitive personal data, which should clearly be enunciated under Regulation 2. This classification, given the 'high risk to the rights and freedoms of data subjects by virtue of its nature, scope, context and purposes' mandates the following: 1. Prior Data Protection Impact Assessments (or **DPIAs**) (Regulation 19); and 2. Prior registration and certification of data controllers with the Data Commissioner; 3. The prior recruitment/appointment of a competent and qualified data protection officer (Regulation 20), amongst others, as prescribed under the Data Protection Act (2019).
General	We recommend the	The comprehensive protection of personal data in Kenya goes hand in hand with the operationalisation

[2] United Nations Statistics Division (2019) 'United Nations Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management' <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi2z8eNofvnAhUlx4UKHUXICkYQFjAAegQIBRAB&url=https%3A%2F%2Funstats.un.org%2Funsd%2Fdemographic-social%2FStandards-and-Methods%2Ffiles%2FHandbooks%2Fcrvs%2FCRVS_GOLF_Final_Draft-E.pdf&usg=AOvVaw0Vn4wgWRXQWjBEv-otbbD0>

Comment 3	operationalisation of the Office of the Data Protection Commissioner	of the Office of the Data Protection Commissioner. We note that (*as at 2 March 2020*) that this office has not yet been operationalised which prevents the coming into force of all provisions under these draft Regulations.
General Comment 4	We recommend that the fees imposed be reasonable, and that all such fees are specified in a schedule. However, there should be no fees for accessing personal information.	Regulations 10 and 13 fail to provide clarity about the amount of chargeable fees. Generally, imposing fees before data subjects can access their personal information (*in any portable format*) prevents the proper implementation of the right to access information under Article 35, Constitution of Kenya (2010). Section 12, Access to Information Act (2016), stipulates that 'no fees should be levied in relation to the submission of an application.' However, where fees must be charged, the 'fee shall not exceed the actual costs of making copies of such information and if applicable, supplying them to the applicant.' This minimal fee should be subjected to the oversight of the Office of the Data Protection Commissioner and the Commission on Administrative Justice (or **CAJ**). Lastly, section 38 (6), Data Protection Act (2019) permits the imposition of 'reasonable' costs, following a data portability request. Notably, international law is strongly opposed to the imposition of fees for access. Article 12, GDPR prohibits most fees, unless the "requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character" or where an individual requests further copies of their data following a request.Under Convention 108, the Explanatory Report states that the principle should be free access and fees should only be imposed in "exceptional" circumstances.

Matrix Presentation

Clause	Provision	Proposal	Justification
Regulation 2	*Interpretation* "authorized user" means an officer or employee of the civil registration entity who is expressly permitted to access the civil registration entity's database and database system	We recommend the substitution of the term "authorised user" with "authorised officer"	The term 'authorised user' is not defined in either the Data Protection Act (2019) or the Registration of Persons Act (CAP 107). However, the RPA (CAP 107) defines the term "authorised officer" which means "a registration officer authorized by the Principal Registrar to exercise the powers or perform the duties and functions in respect of which the expression is used."
Regulation 2	*Interpretation* "biometric data" has the meaning assigned to it under the Act	We recommend amendments to the Data Protection Act (2019) We recommend the imposition of restrictions to the type of biometric data to be collected by CRE's	The current definition of 'biometric data' permits 'deoxyribonucleic acid analysis'. This does not adhere to the restrictions set out by the High Court in Consolidated Petitions No. 56, 58 & 59 of 2019. The High Court orders magnified that the "collection of DNA and GPS coordinates for purposes of identification is intrusive and unnecessary, and to the extent that it is not authorised and specifically anchored in empowering legislation, it is

			unconstitutional and a violation of Article 31 of the Constitution." We propose the collection of biometric data (*subject to restrictions noted above*) should adhere to section 25, DPA (2019). Specifically, the data collected by CRE's must be 'adequate, relevant, (and) limited to what is necessary in relation to the purposes for which it is processed.'
		We recommend the prior and mandatory registration and certification of data controllers and processors with the Data Commissioner	Under section 18, DPA (2019), any entity (including CREs) processing sensitive personal data (including biometric data) must first register with the Data Commissioner. Notably, the collection of sensitive personal data before prior registration and certification constitutes an offence and a violation of the DPA (2019).

Regulation 2	*Interpretation* "civil registration" means the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events to the population including registration of births, adoption, marriage and death	We recommend the adoption of the UN definition of 'civil registration' and propose the insertion of the phrase "as provided by the law".	This is a substantive clause that should be proposed as an amendment to the Registration of Persons Act (CAP 107), and not as regulations to the Data Protection Act (2019). We note that this definition is largely similar to the United Nations (2019) definition, which defined civil registration as "the continuous, permanent, compulsory, and universal recording of the occurrence and characteristics of vital events (live births, deaths, fetal deaths, marriages, and divorces) and other civil status events pertaining to the population as provided by decree, law or regulation, in accordance with the legal requirements in each country."[3] However, it does not include the same to be within the law.

[3] http://www.emro.who.int/civil-registration-statistics/about/what-are-civil-registration-and-vital-statistics-crvs-systems.html

Regulation 2	*Interpretation* "civil registration entity" means a public agency responsible for administering laws under regulation 3, and includes— (a) the National Registration Bureau; (b) the Civil Registration Service; (c) the Registrar of Marriages; (d) the Department of Immigration; (e) the Registrar responsible for Children Affairs; (f) the Department of Refugee Affairs; and (g) the Principal Secretary	We recommend the expansion of this list to include all public agencies and government ministries	We note that this list is not exhaustive and does not capture all public entities involved in the processing and retention of civil registration (personal) data, including the Ministry of Interior and Coordination of National Government (responsible for IPRS), the Ministry of Education (responsible for NEMIS), the National Transport and Safety Authority (responsible for TIIMS), the Kenya National Archives, amongst others.

	responsible for the National Integrated Identity Management System database.		
Regulation 2	*Interpretation* "data controller" means the Principal Secretary for the time being responsible for civil registration;	We recommend amendments to the Registration of Persons Act (CAP 107) We recommend the prior and mandatory registration and certification of data controllers and processors with the Data Commissioner	The Registration of Persons Act provides for a Principal Secretary whose docket is not named. Under section 18, DPA (2019), any entity (including CREs) processing sensitive personal data (including biometric data) must first register with the Data Commissioner. Notably, the collection of sensitive personal data before prior registration and certification constitutes an offence and a violation of the DPA (2019). The Office of the Data Protection Commissioner should be operationalised to ensure proper oversight of data collection programmes.
Regulation 3	*Scope of the Regulations*	Delete Regulation 3 (d)	This is a repetition of regulation 3(c).

Regulation 5	*Privacy in processing personal data*	Delete the qualifying phrase 'necessary information' under Regulation 5 (d) We recommend the operationalisation of the Office of the Data Protection Commissioner	The use of the qualifying phrase 'necessary information' contravenes the Data Protection Act (2019) and the Access to Information Act (2016) by permitting CREs to subjectively determine the type of personal data a data subject can access. This fails to pay proper homage to section 26, Data Protection Act (2019) which places a duty on data controllers to adhere to data subjects' right to access *all* personal data as well as the principle of 'lawfulness, fairness and transparency.' The non-operationalisation (*as at 2 March 2020*) of the ODPC, and the failure of the same to prescribe codes of conduct enables data controllers to operate in direct contravention to Regulation 5 (e).
Regulation 6 and 7	*Consent and Manner of giving consent.*	We recommend the insertion of a subsection recognising data subjects' right to withhold consent and the implications therefrom.	We note that this provision does not recognise the right of data subjects to withhold consent, and neither does it specify the implications for data subjects who opt to withhold consent, and further fails to set out permissible grounds for the same. Notably, section 32 (2), Data Protection Act (2019) caters for the right of data subjects to withdraw consent at any time.

			We therefore recommend that the provision be revised in line with the requirements under section 32(2) of the Data Protection Act.
Regulation 9	*Limitation in processing of personal data*	We recommend the explicit provision of an avenue for appeal Insert a new sub-section, Regulation 9 (5) as follows: "*Where a request for the restriction of personal data has been denied by the civil registration entity, the data subject may, where dissatisfied with the decision of the civil registration entity lodge a complaint with the Data Commissioner.*"	We note that this provision fails to explicitly provide data subjects with any appeal mechanism where a CRE refuses to restrict the processing of personal data. Notably, this requires the prior operationalisation of the Office of the Data Protection Commissioner.
Regulation 10	*Access to personal data*	We recommend the deletion of fees chargeable under Regulation 10 (4)	**See:** *General Comment 4 above.*

Regulation 11	*Rectification of personal data*	We recommend amendments to Regulation 11 We recommend the operationalisation of of the Office of the Data Protection Commissioner	We note that Regulation 11 does not clearly specify what types of documents need to be adduced in support of an application for rectification of persona data by a data subject. This non-specificity is replicated in Form 2 (First Schedule) which calls for the provision of 'any other documentary evidence.' Problematically, this provision assumes that all resident individuals have access to documentary evidence. Further, we note that rectification should not be dependent on the CRE being satisfied about the necessity of rectification. Instead, the Regulations should provide explicit grounds permitting CREsthe ability to deny a rectification request. These grounds should be subjected to the oversight of the Office of the Data Protection Commissioner.
Regulation 13	*Data portability request*	We recommend the inclusion of specific timelines for the processing of data portability requests, in line with section 38 (6), Data Protection Act (2019).	**See:** *General Comment No. 4 above.*

Regulation 14	*Exercise of data subject rights by others*	We recommend amendments to this provision and the transfer of the burden from data subjects to data controllers	We note that Regulation 14 (2) presumes the existence of a relationship 'between the person and the data subject unless evidence to the contrary is adduced.' This fails to acknowledge the security risks of unauthorised third (3rd) parties unlawfully exercising a data subjects' right. We note that data controllers should be obligated to "use all reasonable efforts to verify the identity of others trying to exercise the rights of a data subjects." This is in line with international best practice, under the GDPR. Further, we note that this provision contravenes section 27 (3), Data Protection Act (2019) which stipulates that prior authorisation must be obtained from either the data subject themselves, or a person/body capable of granting prior authorisation on behalf of a data subject.

Regulation 15	*Personal data relating to a child*	We recommend the clarification and alignment of this provision with the Data Protection Act (2019) We recommend the provision of clarity about the type of mechanisms data controllers are mandated to incorporate	We note that this provision is not aligned with section 33 (2), Data Protection Act (2019) which fails to protect the processing of childrens data by data controllers. The rovision requires data controllers to pre-verify two (2) core elements before children's personal data is processed. This includes age verification and consent. Notably, these Regulations fail to provide explicit guidelines about the kind of 'appropriate mechanisms' (e.g., technical standards and specifications) which data controllers are mandated to put in place.
Regulation 16	*Duty to notify*	We recommend the provision of further clarity to this provision	We note that the Regulations fail to provide clarity regarding the practicalities of the notification requirement (i.e., systems and procedures). Additionally, the Regulations fail to set out a format for notification.
Regulation 17	*Retention of personal data*	We recommend the deletion of the retention of processed personal data in perpetuity unless the same is exempted under the Data Protection Act (2019) Regulation 17(1) should state the specific law	The retention of processed personal data 'in perpetuity' contravenes the well-established principle that personal data should be retained for a specific purpose and as long as it is necessary for the purposes for which personal data is collected. The Regulations should adhere to the Data Protection Act (2019)

		upon which the retention is to be done, as opposed to using the phrase "in accordance with the enabling written laws."	and international standards and only permit the retention of processed personal data, where the same is 'reasonably necessary.' Instructively, section 39 (1)(d) permits the retention of personal data beyond 'reasonably necessary' periods where the personal data is for 'historical, statistical, journalistic literature and art or research purposes.' The Regulations should mandate all data controllers retaining personal data under this exemption to maintain an information asset register, which is subject to the oversight of the Data Commissioner. This register should be comprised of the following: clear and accessible 'retention policies or retention schedules which list the types of record or information' held by data controllers, what they will be using this personal data for, and the period of retention for different categories of personal data. Due to the need to balance the right to access information, freedom of expression and privacy, the Data Commissioner should exercise oversight over civil registration entities' ability to formulate administrative mechanisms affecting the deletion, erasure, pseudonymisation and anonymisation of personal data. This is particularly crucial given the need to ensure that the 'journalistic exemption' clause is protected.

Regulation 18	*Notification of breach of personal data*	We recommend the operationalisation of of the Office of the Data Protection Commissioner	The Data Commissioner plays an integral role in ensuring that breach of personal data is adequately addressed. The continued non-operationalisation of the ODPC drastically affects data controllers' duty to notify under the Data Protection Act (2019) as well as data subjects' rights. Nonetheless, the Regulations should clearly impose a requirements on all data controllers to implement clear and accessible breach detection, investigation and internal reporting procedures capable of identifying and redressing instances of breach. Additionally, all data controllers should be mandated to retain a record of all personal data breaches, irrespective of the obligation to notify the Data Commissioner.
Regulation 19	*Data protection impact assessment*	We recommend the deletion of this provision	**See:** *General Comment 2 above*
Regulation 21	*Sharing of personal information with public agencies*	We recommend the deletion of this provision We recommend the operationalisation of of the	This is a substantive amendment that should be proposed as an amendment to the Data Protection Act (2019). We note that the term 'public agency' is not defined in the principal Act, and this provision is *ultra vires.* We note that data sharing should be subjected to the oversight of the Data Commissioner, and is only permissible after comprehensive data-sharing codes have been prepared by the

		Office of the Data Protection Commissioner	ODPC (section 55 (2), Data Protection Act (2019)) and internalised by data controllers. Lastly, the Regulations should require data controllers to proactively disclose the sharing of personal information, and data subjects' should be able to exercise their right to provide, withdraw or withhold consent.
Regulation 22	*Automated individual decision making*	We recommend the provision of amendments to this provision	We note that the duties imposed on data controllers in the Regulations are limited in relation to the right of the data subject when a decision is based on automatic processing. Notably, section 25(b), Data Protection Act (2019) requires data controllers to ensure that personal data is "processed lawfully, fairly and in a transparent manner in relation to any data subject." We note that the Regulations fail to provide the following: a time limit for the provision of notification to a data subject, a format for the provision of notification and a timeline for CREs to respond to a data subjects' request. Further, we note that Regulation 22 (1)(h) fails to provide data subjects' with the right to object to automated processing; the phrase 'express their point of view' is inadequate and does not protect any right.

			International law has stipulated standards that impose duties and rights for the data subject in relation to automated decision-making. Notably, Article 22, GDPR states that a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. It further provides that the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. This is clearly set out under section 35, Data Protection Act (2019).
Regulations 24 - 38	*Part V: Security Safeguards*	We recommend the provision of further clarity to these provisions We recommend the provision of strong and audited encryption methods, which are approved by technical bodies	We note that the Regulations do not prohibit dual use of personal data. We note that Regulation 35 (2) permits (2) CREs to 'transfer personal data from the database through a public network or the Internet shall be conducted by commonly used encryption methods.' While this encourages the use of publicly known security systems, it should be noted that publicly known systems do not provide adequate or strong measures for the protection of personal information.

			We note that encrypting personal data whilst it is being transferred from one public network to another provides effective protection against interception of the communication by a third (3rd) party whilst the data is in transit (i.e., during transfer). Under international law, ensuring the right to respect for informational privacy imposes a special responsibility on the State to apply and utilise new technologies. This necessitates a balancing of the benefits associated with the use of those technologies, and the interference that such technologies place on the right to respect data protection.
Regulation 38	*Transfer of personal data outside Kenya*	We recommend the deletion of this provision	The proposed collection of personal information under this regulations, relates to the personal information of all Kenyans. The nature of this information is such that it should not be transferred outside the country. There is no legitimate basis for such transfer. Secondly, this provision contravenes Part VI of the Data Protection Act as it usurps the power of the Data Protection Commissioner by attempting to grant the National Security Council power to authorise the transfer of personal data outside of Kenya.

About the Partners

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 on behalf of, and 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 and Cybercrime Bills including Uganda's Data Protection and Privacy Act (2019), Kenya's Data Protection Act (2019), the Kenya Cybercrime and Computer Related Crimes Bill 2014, the Tanzania Cybercrime Act, 2015 and the Huduma Bill (2019), 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 contact us at kenya@article19.org or +254 727 862 230.

Kenya ICT Action Network:- The Kenya ICT Action Network (or **KICTAnet**) is a multi-stakeholder platform for people and institutions interested and involved in ICT policy and regulation. The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development. KICTAnet is a space for translating the ideas given by listers into meaningful proposals for resolution of challenges facing the ICT sector.

The network has largely operated as a listserv and, in the last ten (10) years, over thirty thousand five hundred (30,500) messages have been exchanged. There have been over eight thousand (8,000) different discussion threads. Most discussions happened between 2011 to 2013, and again in 2016. Top threads included the *Vision 2030 and misplaced priorities, Hate text messages/KICA section 29, Digital migration and mass ignorance.* Notably, the ICT policy discussions have had the most engagement, with over twenty seven thousand (27,000) exchanges. This confirms that KICTAnet is indeed an ICT policy platform and a reservoir of critical dialogue on matters ICT policy.

If you would like to discuss this analysis further, please contact Grace Githaiga ggithaiga@kictanet.or.ke.