MEMORANDA ON THE DATA PROTECTION POLICY AND BILL
SUBMISSION BY NICHOLAS KANYAGIA AND MARK TUM

Part	Clause	Provision	Proposed amendment
I	2	"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements;	"……. person's race, sex, **sexual orientation** pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion……" Should include sexual orientation to prevent discrimination
	2	"third Party" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data;	"…….other than the data subject, **data subject legal custodian,** data controller, data processor or persons who, under the direct authority of the data controller or data processor,....." Exclude legal guardian from the definition of third party - Third party should effectively act on behalf of the data subject.
	2	"data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;	The bill does not specify the terms of the relationship between the data processor and the controller as in the GDPR https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/
	4(1)(b)	is established or ordinarily resident in Kenya and processes personal data while in Kenya; or (ii) not established or ordinarily resident in Kenya, but uses equipment in the Kenya for processing personal data, other than for the purpose of transit through the country;	Kenyans outside the country for more than 183 days are not covered: - The scope of the bill should be include the processing of personal data of all kenyan citizens regardless of where they reside
	4(2)(a)	This Act shall not apply to the exchange of information between government departments and public	What information is 'need to know' and who determines what is need-to-know? The government departments requesting for the information should also provide detailed explanations

		sector agencies where such exchange is required on a need-to-know basis;	about why they need the personal data, their objective and ultimately they should get consent of the data subject/guardian.
II	6	The Data Commissioner shall be appointed by the Cabinet Secretary on a competitive basis and on such terms and conditions as may be specified in the instrument of appointment.	For independence purposes there should be an independent commision that registers data controllers (if amendment III .1 below is not considered) and enforces regulations rather than having one commissioner appointed by the cabinet secretary. Such as the Independent Commissioner's Office of the GDPR https://www.kefron.com/blog/role-of-the-information-commissioners-office/
	7(d)	promote self-regulation among data controllers and data processors.	Self-regulation beats the purpose of the Data Protection Bill, rather Data Commission should promote cooperation amongst the data controllers and data processors around compliance.
	7(27)(4)	A data controller who contravenes the provisions of section (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five million to imprisonment for a term not exceeding five years	The fine/penalty should commensurate the size of the company, extent of the breach and the extent that the data subjects suffered a loss or injury. https://gdpr-info.eu/issues/fines-penalties/
	8(2)(a)	Without prejudice to the generality of subsection (1), the Data Commissioner shall have power to— conduct investigations on own initiative, or on the basis of a complaint made by a third party;	"conduct investigations on own initiative, or on the basis of a complaint made by **the data subject** or a third party" The complaint can be made by a data subject not just third party
III	15	Subject to exemptions provided under this Act, no person shall act as a data controller or data processor unless registered with the Data Commissioner.	Anyone can be a data controller. We cannot possibly expect everyone to register. We propose that the registration requirement be abolished and instead, controls be taken to address high risk organisations (those who hold a lot of personal data) similar to the GDPR regulations. https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/
	16(3)	A data controller or data processor who knowingly supplies any false or misleading detail under subsection (1) commits an offence.	Define actual punishments of such offences in terms of fines or sentencing.
	16(3)	A data controller or data processor who knowingly supplies any false or misleading detail under subsection (1) commits an offence.	Define who is ultimately liable for a breach in the subjects confidentiality. Is it the controller or the processor or both.

	19	The Data Commissioner may, upon issuance of a notice to show cause, cancel or vary terms and conditions of the certificate of registration where— (a) any information given to by the applicant is false or misleading; or (b) the holder of the registration certificate, without lawful excuse fails to comply with any — (i) requirement of this Act; or (ii) term or condition specified.	A provision to address what happens to the personal data held by the controller when the certificate is withdrawn should be added.
IV	23	A data subject has a right to — (e) deletion of false or misleading data about them.	There should be an addition of the term "deletion" in chapter 2 to define if deletion is only from active systems, if backups are still kept and if so for how long. Also, the bill does not account for the right to request personal data deletion or as known in the GDPR "the right to be forgotten"
	25	(c)the data subject has consented to the collection from another source	This statement is ambiguous. Is the data subject consenting for someone to collect the subject's data from another source or is it that the data subject has consented the other source to collect from them.
	25	(e) the collection from another source would not prejudice the interests of the data subject;	There is need to explain what prejudice in this case and how does it apply.
IV	29(1)	Every data controller or data processor shall process personal data of children in a manner that protects and advances the rights and best interests of the child.	Include a provision that the guardian is fully liable to any acts that may be considered not to be in the best interest of the data subject
IV	38(1)	Where there is a breach of security of personal data or there is reasonable ground to believe personal data has been accessed or acquired by unauthorised person, the data controller or data processor , within prescribed period	the data controller or data processor breach should notify the Data Commissioner within of the breach within 72 hours, failure to which they would have committed an offense https://gdpr-info.eu/art-33-gdpr/
IV		Not provisioned	The data controller is liable for any breach of data and the data subject can sure the data controller to the extent that they suffered a loss including reputational damage
		Not provisioned	The bill does not provide for data protection of deceased data subjects https://gdpr-info.eu/recitals/no-27/