

There were 6 issues up for discussion:	<p>1. Independence of the Data Protection Commission: oversight mechanisms, financial independence</p> <ul style="list-style-type: none"> • The current position: The bill of rights is meant to be enforced by a) the courts or b) Article 59 Commissions. Currently that is the a) KNCHR b) the Commission on Administrative Justice and c) the National Gender and Equality Commission. • The two proposals to oversee the bill are as follows: 				
	Office	Kenya National Commission on Human Rights	The Ombudsman	A new Commission	Corporate Body/ ICT bodies
	Mandate	The KNCHR is seen more as activists than mediators. They point out human rights violations but are not necessarily good with developing solutions.	<ul style="list-style-type: none"> • The Access to Information Act (the ATI Act) already has some provisions about data protection. • This seems to go with the history that the ATI Act was meant to be passed and operationalised alongside the Data Protection Act (the DP Act). However, when the process stalled, the ATI bill continued as a private members bill. • Overseeing both ATI and DP is seen in sectors as overloading the Commission's mandate. • Considered more of mediators than activists. They balance interests and try to find middle grounds and workable solutions. 	<ul style="list-style-type: none"> • A new commission would be a clean slate with a clear mandate and operations. 	Functions defined by Articles of memorandum and the mandate given by the appointing officer.
	Decision making	Appointment of Commissioners and decision making considered	Appointment of Commissioners and decision making considered complex compared to a body corporate.	Appointment of Commissioners and decision making considered complex	Appointment of officials and decision-making is

			complex compared to a body corporate.		compared to a body corporate.	easier compared to a body corporate.
	Perceived institutional Independence	<ul style="list-style-type: none"> The Commission can only be eliminated via a referendum The Commissioners have security of tenure and ideally, can only be removed by a Commission of Inquiry. 	<ul style="list-style-type: none"> The Commission can only be eliminated via a referendum The Commissioners have security of tenure and ideally, can only be removed by a Commission of Inquiry. 			Officials serve at the pleasure of the accounting officer and the body's board.
	Financial independence	Perceived financial independence as an Article 254 Commission.	Perceived financial independence as an Article 254 Commission.		Perceived financial independence as an Article 254 Commission.	Depends on the discretionary allocation from the relevant ministry.
	Cost	Lesser cost to incorporate the new mandate within the existing functionalities.	Lesser cost to incorporate the new mandate within the existing functionalities.	<ul style="list-style-type: none"> Fatigue of appointing yet another institution that will burden the wage bill. May take time to build capacity and buy-in. 		
	Comparative analysis			<ul style="list-style-type: none"> Ghana <ul style="list-style-type: none"> Multi-sectoral (i.e. different govt departments represented in the Commission - not enough commitment.) 	<ul style="list-style-type: none"> Mauritius SA 	
	<p>2. Data Protection Officers: whether, how they should be appointed, functions etc.</p> <ul style="list-style-type: none"> Registration <ul style="list-style-type: none"> It is best to set the bar high for registration then offer leeway for exemptions. It is best to consider tiers for registration through regulations. 					

	<ul style="list-style-type: none"> • Where a firm is not required to register, it should still be made clear to them that they will still be required to comply with the general provisions of the DP law. ○ There should be a clear philosophy on exemptions considering small start-ups are currently handling significant volumes of data; <ul style="list-style-type: none"> • Size, volume, sensitivity of data, sector. ○ The definition of a data subject needs clarification. <ul style="list-style-type: none"> • Does the data subject own the data? Is it the person from whom the data is obtained or whose it is? • Companies will have the option to appoint a data protection officer. <ul style="list-style-type: none"> ○ It may not be necessary for small companies. • The bills need to clarify the differences between a data controller and processor. <ul style="list-style-type: none"> ○ The remedies for the data subject against both the data controller and processor should also be clarified. • It is important to understand that we're legislating for both a formal and informal economy, something, Europe and the rest of the world apart from India do not have to deal with.
	<p>3. Digital Identities: Biometrics, NIIMS, Alternative Credit Scoring (ACS)</p> <ul style="list-style-type: none"> • Digital identities are promoting financial inclusion and merging technologies such as smart services, IOT, blockchain etc. <ul style="list-style-type: none"> ○ Case study of Estonia ○ However, these jurisdictions have proper security infrastructures compared to our situation. <ul style="list-style-type: none"> • Consider the CIPIT report on the privacy implications of applying biometrics to Kenya in 2018. • Consider the data breaches on the Aadhaar system. • Biometrics <ul style="list-style-type: none"> ○ Considered excessive and against the principle of data minimization ○ Health sector - biometrics considered vital for identification where there is duplication of names <ul style="list-style-type: none"> • There is a push back that other less intrusive unique identifies can be deployed in this situation. • Study by KELIN - guarantee had to be given that biometrics stored as encryption not image. • Portability and access. <ul style="list-style-type: none"> ○ Firms will be required to update their systems to allow for proper infrastructure for ID verification and data portability. ○ Most of the fintech firms are ready for porting compared to situation in TZ and UG. • Presentation on ACS; <ul style="list-style-type: none"> ○ Micro-lending entities using Call Detail Records (CDR) and Customer Relationship Management (CRM) ○ Some of this data is personal and could be challenged once the DP regulation is in place. ○ There is need for more transparency on the categories of data used and how the data is used. ○ The eventual Act could do away with scams ○ There's more work needed to ensure the right to be forgotten is implemented ○ Removal of personal data will affect the loan affordability criteria - without much data the risk level goes high. ○ There's more research needed on the type and quantity of data that should be permissible for use in these apps.

	<ul style="list-style-type: none"> ○ The eventual framework should prescribe the opt-in mechanisms that should be availed by these apps. ○ A user should have enough awareness on the impact the choice they make to share their data will have. ● Profiling versus automated decision making. <ul style="list-style-type: none"> ○ The distinction should be made clear and the recognition that humans too have systematically used data to discriminate e.g. housing in the US. <ul style="list-style-type: none"> ● So, it's not about machine algorithms but the oversight on the decisions made using such data.
	<p>4. Limitations: philosophy, scope & limitations</p> <ul style="list-style-type: none"> ● Section 6 senate bill ● Section 48-50 Taskforce bill ● Subject matter - National security tax ● The senate bill exempts institutions while the taskforce exempts actions. ● The exemption philosophy is not clear <ul style="list-style-type: none"> ○ Section 49 - research purposes exempted indefinitely <ul style="list-style-type: none"> ● Note the CA scandal started with research data ○ Section 6(3) senate almost wholly negates the law ● There should be a clear philosophy for limitations <ul style="list-style-type: none"> ○ Consider the 13 principles - https://necessaryandproportionate.org/principles ○ These principles should be translated into proper legislative equivalents.
	<p>5. Cross-border transfers: sovereignty versus residence</p> <ul style="list-style-type: none"> ● Consider that the law is a tool to balance interests. ● Why should we localize? <ul style="list-style-type: none"> ○ Do we have the appropriate infrastructure for cloud services? <ul style="list-style-type: none"> ● Data centre tiers https://www.colocationamerica.com/data-center/tier-standards-overview.htm ● Skills ● Resources e.g. guaranteed security, electricity. ○ What are the criteria for localization? <ul style="list-style-type: none"> ● Consider target jurisdictions may have stronger data protection laws than we currently have. <ul style="list-style-type: none"> ▪ Will they apply to our data? ○ Health Information Policy and E-health strategy have already determined that health data should be processed locally. ● Will the eventual act have extra-territorial jurisdiction? <ul style="list-style-type: none"> ○ How do we enforce this? ○ Our security laws are bordered while tech is borderless. ● How do you ensure control? <ul style="list-style-type: none"> ○ Current mutual legal assistance frameworks are inefficient

	<ul style="list-style-type: none"> ○ There is a research need to strengthen this. ● Intermediary liability <ul style="list-style-type: none"> ○ Hosting a 3rd party service, notice to takedown - are these effective?
	<p>6. Transition & Implementation: allowance to migrate systems and compliance.</p> <ul style="list-style-type: none"> ● Research need - to increase awareness of the rights that will be brought by the new law. <ul style="list-style-type: none"> ○ GDPR took 5 years to implement ○ Ghana took 2 years to implement. ○ Kenya? <ul style="list-style-type: none"> ● Setting up the Commission/Body will take a min - 3 months (appointments) ● Post set up, the Commission/Body will need time to build capacity (Human Resource, technical capacity) - 6 months. ● post promulgation, the Commission will need time to promote awareness (campaign, registration) - 6-12 months ● It would be important to implement both a delayed effective date and phased implementation of the eventual Act; ● There is research needed to identify what needs phasing. <ul style="list-style-type: none"> ○ Consider SME needs. ○ Consider the needs to awareness amongst the public. ○ Consider the needs to build capacity within the DP Commission/Body. ○ Consider time for systems migration <ul style="list-style-type: none"> ● Security ● Portability ● Balancing interest - human rights versus national security versus innovation (convergence) <ul style="list-style-type: none"> ○ Need to harmonize between existing institutions. <ul style="list-style-type: none"> ● There is need for more research on the basis from which this should be done.