The Clerk of the National Assembly

P.o. Box 41842 – 00100

Nairobi Kenya

SUBMISSION OF MEMORANDA FROM KICTANET

Data Protection Bill – Proposed amendments from the Kenya ICT Action Network

We wish to submit the following recommendations for amendment of the Data Protection Bill. While overall we are highly supportive and enthusiastic as to the positive impact of the Bill, there are several provisions that if left as is could negatively impact innovation in the technology and finance sectors, and hinder both competition and consumer rights.

Generally, it is a good bill that is well improved compared to previous versions. For example, the object of the proposed law is positive as opposed to previous versions that included exemptions in the objects. There are also fewer limitations on the right to privacy.

There could be further sharpness on engagement of data subjects with data controllers and processors. There are several clauses that propose response to the the data subject "within a reasonable period". While the rationale behind this is to ensure that data processors can continue with their core business even where there are numerous requests, there should be a better balance between business interests and data subject right to information.

SPECIFIC PROPOSALS:

Section	Clause	Proposed Amendment	Concern
28 Collection of personal data	"personal data may be collected indirectly where— (e) the collection from another source	Remove sub-section 28(e) in its entirety	▪ This exemption is difficult to interpret and enforce. It does not specify who determines what is prejudicial to the interests of the data subject. This could create a legal loophole where firms or their partners determine what "prejudice" is in a broad manner, and use this to

	would not prejudice the interests of the data subject."		justify improper data collection without informing consumers. ▪ This standard and provision is far too open to interpretation by the data controllers, and would require substantial supervisory resources to ensure this loophole is not improperly abused. It is better it is omitted as it is likely to create more problems/challenges than it is attempting to address.
34 Restrictions on processing	"(2)(b) the data controller shall inform the data subject before withdrawing the restriction on processing of the personal data."	Change "inform the data subject" to "obtain consent from the data subject"	▪ A data controller should not be allowed to remove a restriction on processing of information without getting consent from the data subject to do so, not just informing them they are doing so. ▪ A data controllers could simply send an email that they have decided to process their data in a way not previously authorized by the customer, and not have to seek approval from this customer to do so.
38 Data portability	"(6) A data controller or data processor shall comply with data portability requests, at reasonable cost and within a period of 30 days."	Remove clause (6) in its entirety and replace with the following: "The Data Commissioner shall coordinate with relevant authorities across industries to enact rules and guidance for data portability for different types of data collectors and data processors that reflect the following objectives: -Timeliness of data subject access -Ease of data subject access -Ease of understanding of data -Ease of portability -Security of data -Fair competition -Cost to data collectors, data processors and data subjects	▪ This clause as constructed will make consumer-led information sharing in key sectors like technology and financial services completely unworkable. If data controllers are given 30 days to give consumers access to things like their financial information, this would kill the possibility of many data-driven technology services that rely on near real-time analysis of data to provide customized and lower cost services to consumers. . ▪ The clauses as currently drafted runs counter to our experiences of what does and does not work with regards to consumer-led information sharing. This statute will tie the hands of sector regulators wishing to implement information-sharing regulations that are custom-built to their industry which would require faster exchange of information. For example, this week Central Bank of Kenya highlighted Open Banking at the Afro-Asia Fintech Festival. Yet Open Banking relies on near-instant consumer sharing of their accounts across

			providers, and this law would prevent that from being mandated by Central Bank of Kenya or other actors. ▪ The replacement of "free of charge" from the July 2018 draft with "reasonable cost" is a related concern. Dominant actors will practice discriminatory pricing and excessive margins to assist partners and hinder rivals in areas like USSD or payments interoperability—both of which already required the intervention of CAK and CBK, respectively. If "reasonable cost" is included, it is likely a similar bad practice will emerge and financial regulators will have to intervene to address discriminatory pricing and consumer fees to access their own financial information. This will empower more banks to charge for their account statements, even if they currently provide them for free, as it legitimizes such practices. ▪ Finally, because consumers' rights to access their information—without portability—is included in this section, but not further defined elsewhere, the section appears to say that firms can also take 30 days and charge a fee to even simply give a consumer records. This means firms could now needlessly delay consumer access to things like account statements, medical records or other information vital to their economic and personal lives. ▪ The potential damage of Section 38 as currently drafted on Kenyans control of their data, as well as provider competition and economic innovation is substantial, and so we strongly recommended a full revising of this section along the lines recommended above.
Section 50	Processing through a Data Server or Centre in Kenya	Modify the Clause. Clear guidelines are required on the criteria that will be used to make a decision on the data that stays local,	▪ Gives the CS unilateral powers to decide which data enterprises must process data locally. ▪ Discretionary powers can be open to undue influence and might be misused.

		that way Investors know upfront the parameters of engagement and will not be victims of future suprises.	
General Comments			▪ Is the law tight enough to discourage a scenario in which Kenya is subject to foreign laws and regulations such as GDPR

Clause	**Recommendation**	**Rationale**
29. duty to notify	Clarify that where it is not possible to notify data subject before data collection, controller still has a duty to notify even after collection	Data subjects should be made aware when their data is being collected and processed
29. duty to notify	Create offence where controller fails to notify data subject	Inculcate a practice of notifying data subjects
31. data protection impact assessment	**Question:** Should a DPIA be independent or are there instances when a DPIA should be carried out independently?	
38. data portability	Reduce the reasonable time required for porting requests from 30 days to 14 days	To make portability rights meaningful and in line with the fast moving world of tech
39. data retention exemptions	**Question:** How do we ensure that research is not used to retain data perpetually? How can we also gain from such data- should the law	

	provide for open research/ sharing of research findings openly?	
40(3) right of rectification and erasure	Specify the reasonable time under 40(3) to 14 days	To create a culture of informing data subjects of matters concerning them in a timely manner
43(1) notification and communication of breach	**Question:** Does anyone else find "real risk" ambiguous?	
43(1)(b) notification and communication of breach	Specify "reasonable time" for communication of breach to data subject to forty eight hours	Notification of breach to data subject should be among the issues considered by DPC when receiving reports of a data breach from a processor
46 processing of health data	Provide for Cabinet Secretary to make regulations on processing of health data	There are unique issues in the health sector that may require special regulations
48 conditions for transfer out of Kenya	Make 48(1) (b) and (c) subject to (a)	As an inbuilt measure for adequacy of data protection in jurisdiction where data is transferred
50 processing through a data server or data centre in Kenya	Specify or limit instances where Cabinet Secretary may direct processing in Kenya	To avoid situation like DTB in Tanzania
51 (2) (b) general exemptions	Delete clause 51(2) (b) – necessary for national security or public order	It is ambiguous. Also, 51 (2) (c) covers National Security laws which can specify instances when data may be disclosed
52 Journalism, literature and art	**Question:** An opportunity to ask for open research or making	

	such research free for public consumption?	
53 research, history and statistics	Add clause requiring such research to be open for public consumption	
54 exemptions by Data Protection Commissioner	Require such exemption to be subject to public participation	
70 Annual reports	Redesign clause to require DPC to report to public and Parliament and not Cabinet Secretary	Enhance independence of DPC and eliminate redundancy of CS since CS's role is to transmit the reports to Parliament
75 consequential amendments	Add Registration of Persons Act	It is the greatest collection of personal information and is subject of litigation