KCB BANK KENYA LTD: COMMENTS ON PROPOSED PRIVACY AND DATA PROTECTION POLICY 2018

No.	SECTION REFERENCE	OBSERVATION	RECOMMENDATION
1.	4. Scope 4.3	Access of data especially by government agencies should be clearly highlighted in this policy.	By this policy, revenue collection agencies e.g. KRA should be restricted from demanding customer information unless a clear process of accessing data held by another party. Process should include obtaining a court order or seeking arbitration before data is provided
2.	4. Scope 4.5	4.5 is missing	Correct numbering
3.	4. Scope 4.4/4.6	The policy does classify data	The policy should have clear data classification methodology that categorizes data into various types, forms. This will aid the determination of what can be disclosed and what cannot be disclosed.
4.	5. Principles For Data Protection 5.3 Data Minimization 5.3.3	Behavioural data is collected in advance. This this illegal?	The policy should define “advance” Policy should consider how behavioural data maintained by organisations can be used.
6.	5. Principles For Data Protection 5.4 Storage Limitation 5.4.1	The policy has not defined key words	The policy should define “Longer periods”, “period” and state who determines this period
7.	5. Principles For Data Protection 5.5 Accuracy 5.5.1/5.5.2	Change in personal data details may be out of control of data controller e.g. telephone number, address	Incorporation of data classification into policy will remove vagueness
8.	7. Legal Grounds For Processing 7.5 Cross Border Transfer	This clause does not give clear direction on data being used across the country’s boarders	Policy should state that data can only be shared/transferred/stored/processed in countries with adequate data protection policies/standards/laws

9.	8. Obligations For Data Processing 8.2.4	The policy does not provide a format and mode keeping records	Policy should provide format and mode of keeping data
10.	8. Obligations For Data Processing 8.1.11/8.1.12	8.2.11/8.2.12 are missing	Correct numbering
11.	8.5 Data controller must manage any personal data breaches promptly and appropriately:	The reporting requirement is vague	The policy should define the word "expeditiously" Policy should advice number of days to report rather than being vague
12.	9. Institutional Framework	The policy creates a new and additional data protection regulator	Compliance to the policy should be under Communication Authority of Kenya

KCB BANK KENYA LTD: COMMENTS ON PROPOSED PRIVACY AND DATA PROTECTION BILL 2018

No.	SECTION REFERENCE	OBSERVATION	RECOMMENDATION
1	Part II – Office Of Data Protection Commissioner Clause 7 Functions of the Data Protection Commissioner	The draft bill gives sweeping powers to the Data Commissioner.	In clause 7 (b) one of the functions of the Data Commissioner will be to establish and maintain a Register of data controllers and data processors. Almost every business entity in one way or the other will fall under the definition of either a data controller or a data processor which means that this proposed office will have records and a level of over the activities of the entities falling under the two definitions. In clause 7(c) another function of the Data Commissioner is to exercise control on all data processing operations, either on its own motion or at the request of a data subject, and to verify whether the processing of data is done in accordance with the proposed law. Clause 8 of the proposed law gives the Data Commissioner powers to investigate, issue summons to witnesses as well as to request for information, explanation and assistance from any person subject to the proposed law. The above clause also gives the office

			of the Data Commissioner to facilitate conciliation, mediation and negotiation on disputes arising from the proposed law. The proposed laws also gives the Data Commissioner the powers to impose or delegate any of the powers under the law to:- - an employee of the office - a recognised self-regulatory organization - a regulator or professional body - any other public body established through an act of parliament The above proposed powers will make the office of the Data Commissioner very powerful with the discretion on how to handle disputes under the proposed law. The powers mirror those of the police and the office of the director of public prosecutions under one regulation. Furthermore, the Data Commissioner may also facilitate mediation, conciliation and negotiations of disputes. The main problem with this clause is that the circumstances under which this should apply are not clearly defined. It is unclear as to criteria will be used to determine whether a complaint should be treated as a dispute worth being mediated or when a harder stance should be taken. Such ambiguity gives unfettered powers which may be subject to abuse.
2	Part III – The Registration Of Data Controllers and Data Processors Clause 15 Registration of data controllers and data processors.	Requirement of a registry	Under clause 15 of the proposed law no person shall act as a data controller or data processor unless registered with the Data Commissioner subject to exemptions under the proposed law. As earlier mentioned a broad definition of the two terms has been given therefore every business entity or a person engaged in business in one way or the other will fall under the definitions. This creates an unnecessary repository of data in regards to almost all activities being carried out in the country. In addition the information details required during the application made to the Data Commissioner in clause 16 (2) are quite detailed.

	Clause 16 Application for registration.		The details including a description of the personal data, purposes for which it will be processed, possible recipients of the data and the name of the country where the data controller may transfer the data. The registration of all data controllers and data processors is entirely unnecessary. Almost every business entity and individual handling personal data will be subject to the proposed law meaning that they will all need to the register with the office of the Data Controller. A more efficient approach towards the regulation of personal data would be for the office of the Data Controller to only interact with regulated individuals and entities during random compliance checks and following complaints by data subjects. The registration certificate then becomes an unnecessary requirement. The justification for this provision is that the regulator would like to have visibility over whom it is regulating. The provisions for registration in their current state create a clumsy legislation akin to creating a parallel public register. A threshold could be given for registration depending on the number of data subjects an entity or individual handles. The most relevant registry would be that of data protection officers such that when there is a query in regards to compliance, the office of the Data Commissioner will be able to ensure basic compliance.
3	Part VI.- Transfer Of Personal Data Outside Kenya Clause 44 Rule as to data centres and servers	Transfer of data outside Kenya	The provisions in regards to the transfer of data out of Kenya create a difficult business environment for business entities wishing to offer services from outside the country, including the cloud computing industry. Under clause 44: “Every data controller or data processor shall ensure the storage, on a server or data centre located in Kenya, of at least one serving copy of personal data to which this Act applies. (2) The Cabinet Secretary shall prescribe, based on grounds of strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data centre located in Kenya.

			(3) Cross-border processing of sensitive personal data is prohibited." There needs to be a concerted and deliberate effort to ensure the amendment of the above clauses. With modern technology like cloud computing it is possible to ensure the sovereignty of data even when the data resides in another jurisdiction. The only consideration for the transfer or processing of data outside of Kenya is if the adequate security considerations with respect to the protection of personal data are met. Under the proposed law in clause 45(b) the data subject must give explicit consent to the transfer of data having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards. This clause will make cross border data movement operationally cumbersome by requiring prior consent. Furthermore it wrongly presumes that cross border data protection is unsafe from the onset. Clause 46(2) gives the Data Commissioner the power to prohibit, suspend or subject the transfer to such conditions as may be determined. The above provisions in regards to cross border data transfer indicate an inherent misunderstanding over the current technological developments in regards to data residency and immediate interventions must be undertaken to ensure that these clauses are adequately amended.
4	Part VII— Exemptions Clause 47 General exemptions	Cabinet Secretary's powers under the proposed law	The Cabinet Secretary has the powers to offer exemptions to the proposed law through the issuing of a certificate under clause 47 (3). The Cabinet Secretary in clause 50 also gets further powers to prescribe instances where compliance with certain provisions of the proposed law may be exempted. clause 44 the Cabinet Secretary can make a decision on categories of personal data known as critical personal data which can only be processed in servers or data centers located in Kenya.

			- In clause 60 the Cabinet Secretary may prescribe regulations for to govern the certification program under the proposed law. - In clause 61 Cabinet Secretary may make Regulations for the better carrying into effect the provisions of the proposed law. This includes the following :- i) requirements which are imposed on a data controller or data processor when processing personal data ii) the contents which a notice or registration by a data controller or data processor should contain iii)information to be provided to a data subject and how such information shall be provided iv) the levying of fees and taking of charges v) issuing and approval of Codes of Practice and Guidelines vi)any other matter that the Cabinet Secretary may deem fit. The above powers granted to the Cabinet Secretary under the proposed law have a direct impact on the activities of the office of the Data Commissioner and will definitely have a negative impact on the expected independence of the proposed office.
5	General comments	Deficiencies in the proposed legislation.	1. The proposed law makes a provision for the appointment of Data Protection Officers. There is a critical skills gap in the country as people who are equipped to execute the above mandate are few. There should be a transitionary period before the full implementation of the law to allow for capacity building. 2. The current definition of data controller and data processor mean that every entity in Kenya will require strict adherence to the law. There should be tiered levels of responsibility based on the amount or type of data an entity handles.