Data Protection Bill 2018 Public Comments Submission

FSD Kenya

September 12, 2018

We are pleased to submit our comments to the draft Data Protection Bill released by the Ministry of ICT. We applaud the Task Force for their thorough and forward-looking approach to this important subject matter. We believe that this Bill if put into Law will go a long way to addressing problematic practices with data privacy and protection in sectors such as financial services—where FSD Kenya's focus lies.

Our comments are intended to support and enhance this strong draft. They primarily focus on recurring ambiguities and exemptions that we think may limit the effectiveness of this Bill. Many of these include vague language like "reasonably practical" that invite creative interpretation by a data controller's legal team and could undermine the spirit of the Bill. We hope that you will consider these recommendations and perhaps remove those vague provisions and exemptions, as they will also make enforcement of the Bill more difficult and evasion of compliance a risk.

We would welcome any follow-up as needed, and ask that if there are public events or meetings we be considered for invitation as this law would have significant impacts on financial sector policy and provision of financial services.

On behalf of FSD Kenya,

Rafe Mazer
Regulation Consultant
rafe.mazer@fsdkenya.org

FSD Kenya Comments on draft Data Protection Bill 2018

1. **Section 2 Definitions** The functions of the Data Processor and the Third Party require clarification, as they both process data and appear to overlap in part. The definitions have that both could process data under the direction of the Data Controller, and so seemingly in some instances an entity could be both? It would be good to clarify what is different about processing "on behalf of" versus "under the direct authority of" the Data Controller, so we understand how these two definitions are distinct.
2. **Section 3(c)** Recommend adding Specification of Purpose language in the objectives, as it is complementary to minimization and specified in 22(1)(c). Also consider adding an objective related to data subject access to and control of their personal data, as that principle is clear throughout the Bill.
3. **Section 4(2)(a)** What does "need-to-know basis" mean in this context? This seems vague which opens up risk to abuse of this exemption to the Act and its provisions.
4. **Section 7(1)(d)** The specific call out for self-regulation should be considered with caution, as the track record of self-regulation in sectors like financial services is very poor. Overall we do not normally recommend that approach to oversight and suggest reconsidering this strategy. Similarly, under 9(1)(c) what is the official process for determining "a recognised self-regulatory organisation"?
5. **Section 7(1)(g)** Why is the power of inspection limited to evaluating only the processing of personal data? The power should be for all matters related to the provisions of this Bill.
6. **Section 22(1)(f)** Will this be able to accommodate rules for record keeping, such as in banking?
7. **Section 22(h)** How will "adequate" be determined? Should they have equal or greater provisions to this Bill? Or is it a judgement call made by the Commissioner.
8. **Section 23** Should include rights to consent before collecting as well as be informed.
9. **Section 25(2)(c)** This clause would allow a third-party to collect data from a firm without the consent of the data subject to share such information. This should be struck, as it goes against the language regarding notification, consent, and specification of purpose in the Bill.
10. **Section 25(2)(e)** "Would not prejudice" is vague and invites loopholes for not complying with the spirt of the direct collection. Who determines whether it is prejudicial or not? An dhow is the data subject even aware the data has been collected so they may determine if they believe they are prejudiced. This should be struck from the Bill.
11. **Section 25(g)** Similar to other comments on 25, "reasonably practical" is vague and invites attempts to not honor the spirit of the law or seek loopholes. This should be struck from the Bill.
12. **Section 26(1)** "In so far as practical" is vague and invites data collectors to not adhere to duty to inform the data subject, and then just wait to be challenged on this before obeying the law. This could cause widespread abuse of the duty to inform principle. "In so far as practical" should be removed from that sentence.
13. **Section 27(1)(a)** Here it may be helpful to cross-reference that such consent must comply with the principles of Section 26—assuming that the amendments above on 26 are made to close potential loopholes.
14. **Section 27(1)(b)(iii) and (vii)** are not clear how they will be defined. Recommend removing language or clarifying what this means and how it will be determined.
15. **Section 27(4)** For fines, this would be a very insignificant amount for large firms and not much of a deterrent. Overall for fines and sanctions setting a minimum but also allowing for up to a

percentage of annual turnover may have more power as a deterrent for large firms, who are often those holding the most sensitive data for millions of Kenyans, where things like a data breach will have the widest reaching consequences.

16. **Section 30(1)** Recommend replacing "may" with "shall" so that they may not turn down a data subject's rightful claim to restrict processing of personal data.
17. **Section 30(2)(b)** Replace "inform the data subject" with "obtain consent from the data subject" as informing is not enough, data subject must actively and clearly consent. This is a recurring issue in the Bill and we recommend reviewing all cases where duty to inform is required and add in consent requirements.
18. **Section 32** Will the data controller or data processor in this case have to first prove these grounds, and in the interim stop processing at the request of the data subject? This should be made clear, so it is not interpreted that the data controller or data processor can deny such a request, and the then only have to reverse this if that is challenged by the data subject and it is deemed to not be a compelling legitimate grounds. Burden of proof should not be on the data subject in these cases.
19. **Section 33** In this section a provision should be added to require that the data subject actively opts into receiving direct marketing, and that this is separate from adherence to other conditions. You will notice that in much of online commerce this requirement is having a positive impact in terms of marketing assent not being pre-ticked and this principle should be applied in Kenya as well to derive the same benefits for consumers.
20. **Section 34(3)** How will technically possible be determined? We understand the principle behind this—it's not reasonable to have some microenterprise port data digitally—but would propose an alternative approach: Give the Commissioner the ability to determine exemptions to the transmittal requirement due to technical feasibility, size of firm, relative cost to the firm, and other criteria. Also it would make sense to specify the Commissioner may issue rules related to Section 34 overall, so that you obtain maximum flexibility since data portability will play out very differently by segments of the economy.
21. **Section 34(4)(b)** When would sharing of a data subject's personal data by their own request adversely affect the rights and freedoms of others? The rights of a subject for information solely concerning themselves should not be bound by others and their perception of how it affects their rights and freedoms. Recommend striking this provision.
22. **Section 34(5)** Instead of putting one month, we recommend a general requirement for timeliness, and the power to set rules for maximum time by type of data controller/data processor and data type. Consider financial services: 1 month for porting would kill the competitive impact of data portability for lending, as it is too long to wait to make a decision on lending. Strongly request that this one month rule be removed as if it is included in this law it will adversely affect the objectives of competition and consumer protection in financial services and perhaps other industries. Better to set the time periods by sector instead in future rules.
23. **Section 35(1)(b)** What does this clause mean? It seems ambiguous. Suggest removing.
24. **Section 36(2)** It may be useful to require they data controller inform the data subject the names and contacts of all firms they have notified, so the data subject can follow-up with them to ensure rectification or erasure is satisfied by the third party.
25. **Section 47** If the recommendations to add to the objectives 3 are accepted then should be updated here as well.

26. **Section 59** Five million would be a very insignificant amount for large firms and not much of a deterrent. Overall for fines and sanctions setting a minimum but also allowing for up to a percentage of annual turnover may have more power as a deterrent for large firms, who are often those holding the most sensitive data for millions of Kenyans, where things like a data breach will have the widest reaching consequences.
27. **General Comment** There should be a clause requiring separation of product acquisition and consent to data sharing with third parties. 28(3) comes close to this but could be made more powerful. This would require that consent to data processing must be separate from other terms and conditions and not a pre-condition to acquiring a product or service—avoiding the "take it or leave it" commonly used. This both allows consumers not to be forced to sacrifice privacy to acquire products and services, and also puts greater obligation on the firm to demonstrate why they need to process data to benefit the consumer's experience with the product or service in question, supporting the specificity of purpose and minimization language already contained within the Bill.
28. **General Comment** Liability of data controllers. In particular, data controllers should be held liable for breaches by data processors they share personal data with. This will help to ensure that any contracts they have with data processors comply with data protection law. This also speaks to the need to develop separate data controller and processor definitions noted in the comments below.
29. **General Comment** Consent archives. Data controllers should be required to keep processing records of all data transfers to processors so that data subjects may easily identify all data sharing that has occurred, to help with processes such as accessing records or deleting records.