SAFARICOM PLC'S SUBMISSIONS ON THE DRAFT PRIVACY AND DATA PROTECTION POLICY AND BILL, 2018

Schedule 1: Submissions on the Draft Privacy and Data Protection Policy

	Article	Provision	Proposal
1.	2-Purpose of the Policy	2.3 Add new clause to the objectives of the policy	We propose the inclusion of an additional objective aimed at creating a comprehensive data protection environment. Our proposed wording is as follows: "*2.3.6- To establish a framework for ethical use and management of data to facilitate innovation*"
2.	4-Scope	4.2-This policy shall be the overarching guiding policy in relation to matters of Privacy and Data Protection.	The purpose of the Policy is to specifically address Data Privacy and Data Protection. We propose to insert the word "*Data*" immediately before the word Privacy
3.	4-Scope	4.4 This policy applies to any Personal Data, which is processed or controlled by a data controller in Kenya or outside Kenya that processes personal data using a data processor inside Kenya. 4.6 The policy applies to all data subjects, whether resident in Kenya or not, whose data is or has been collected or processed by a data controller in Kenya.	Certain aspects of data protection and privacy are covered in other jurisdictions but with an extra-territorial application. The policy should be clear on what happens when there is conflict of the said legislation. For instance, where the European General Data Protection Regulation (GDPR) may be in conflict with the local data protection framework. We further propose that the policy be amended to extend its application to instances where the data subject is Kenya (regardless of where the data processing takes place).
4.	5-Principles forData Protection - Fairness, lawfulness and transparency	5.1.3- Personal data will be considered to have been obtained fairly if the data subject is informed of the name of the data controller and the purpose(s) for processing the personal data or any further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair.	It might not be reasonable for a data controller to list all uses that the data may be subjected to, especially in the ICT industry with rapid technological advances such as network and system upgrades that impact data processing. This includes application platform upgrades, Internet of Things (IoT). We therefore propose that the clause be amended by removing the word "*specific*". Please note that the principle on transparency will still ensure that data subject is made aware of any additional uses of their data.

	Article	Provision	Proposal
5.	5-Principles forData Protection-Accuracy	5.5.2- Suitable steps must be taken by data controller to ensure that inaccurate or incomplete data is deleted corrected, supplemented or updated.	We propose that the policy be amended to oblige data subjects to provide accurate personal information. The obligation to verify and guarantee accuracy lies with the data subject since it is their data that a data controller is collecting and processing. Nonetheless, a data controller's should provide avenues for data subjects to verify and update their data. Where the data controller or data processor has reasonable doubts about the identity of the individual making the request for deletion, correction or rectification of data, they should be able to request for additional information to enable them to confirm identity. There should also be provisions to allow the controller/processor to delay the request until the identity of the individual is confirmed.
6.	6- Data Subject Rights	6.1 There may be limitations on data rights of data subject when required by the law or when there are competing rights and therefore would require an assessment based on the facts and circumstances.	The Policy has not addressed instances where limitations of data rights can be applied. These should be clearly defined to avert ambiguity or any potential abuse of this clause.
7.	8- Obligations for Data Processing	8.5 Data controller must manage any personal data breaches promptly and appropriately: 8.5.1 All data breaches are to be reported to the Data Protection Regulator. The reporting must be done expeditiously. 8.5.2 The frequency and severity of the breach will determine the next level of intervention.	The time period within which a data breach should be reported as well as a threshold of the data breaches to be reported should also be established. It is envisaged that the kind of data breaches to be reported are those that have the potential to expose the data subjects to harm. This may be discussed further for incorporation into the proposed Regulations.
8.	9- Institutional Framework	9.1- Office of the Data Protection Regulator	We recommend that the establishment of this office precedes implementation of the policy and Bill.
9.	12- Implementation	N/A	The framework should provide for transitional provisions and an implementation framework that provide for, among other things the requirement that the Regulations come into

	Article	Provision	Proposal
			force after the Office of the Data Protection Regulator has been set up.

Schedule 2: Submissions on the Draft Privacy and Data Protection Bill 2018

	Title/Reference	Provision	Comments
1.	Definitions	The term **"Recipient"** has not been defined.	It needs to be clear to whom data is disclosed, whether it refers to a third party or not.
2.	Definitions	"**Sensitive Personal Data**" means data revealing the natural person's race, health status, ethnic social origin, political opinion, belief, personal preferences, location, genetic data, biometrics, sex life or sexual orientation, personal financial expenditures, of the data subject;	Strike out "*personal financial expenditures*" from the definition.
3.	Application	S. 4 (2) (a)–This Act shall not apply to – the exchange of information between Government departments and public sector agencies where such exchange is required on need to know basis	We propose that this clause be deleted. Any processing between Government departments ought to be sufficiently addressed within the exemptions enumerated in Part VII of the Bill.
4.	Registration of Data Controllers and Data Processors	S.16 (1) A person who intends to act as a data controller or data processor shall apply to the Data Commission in the form provided for.	There is need for Regulations to be formulated to define the time periods for the registration process. This extends to all provisions of the Bill where time periods are subscribed. To this end, we propose that the registration certificate be perpetual. The provision should also address the compliance timelines for existing data controllers.
5.	Compliance and Audit	S. 20 The Data Commissioner may carry out periodical audits of the systems held by the data controllers or data processors to ensure compliance with this Act.	We propose that the Bill be amended to indicate that the details on this section will be prescribed in Regulations. These include:- - how often the audits of the systems will be carried out; -how much notice will be given to data controllers or data processors before the audit is conducted;

			- the information that will be subject to audit, to enable the data controller or data processor to avail it in good time; and -the period within which the Data Commissioner should submit the findings of the audit to the data controller or data processor.
6.	Principles of data protection	S. 22 (1) Every data controller or data processor shall ensure that personal data is e) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;	A data controller or data processor is not in a position to determine that personal data is accurate, up to date and not misleading. The Bill should impose additional responsibilities on the data subject to ensure that they provide accurate personal data immediately notify the data controller or data processor there is a change in their personal data.
7.	Processing of personal data relating to a child	S.29 (3) The Data Commissioner may appoint as guardian of the child a data controller or processor who— (a) operate commercial websites or online services directed at children; or (b) process large volumes of personal data of children.	The Bill should include a definition of ***"guardian"*** which will include other relevant parties who are capable of operating independently. Data controller or data processor may not be appropriate guardian.
8.	Data Portability	S. 34 (1)-A data subject has the right to receive the personal data concerning them, which the data subject has provided to a data controller in a structured, commonly used and machine-readable format. (5) A data controller or data processor shall comply with data portability requests, free of charge and within a period of one month. (6) Where a data controller receives a subjects data portability requests, the data controller shall	There is need for an interoperability standard to be defined to facilitate data portability requests. For numerous complex requests consideration should be made for "reasonable costs" as this places a financial burden on data controllers. The request for data portability by a data subject should be subject to reasonable fee.

		provide such data in a structured commonly used and machine readable form.	
9.	Right of rectification and erasure	S. 36 (1) A data subject may, subject to exemptions under this Act, request a data controller or data processor to— (a) rectify personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading; or (b) erase or destroy personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.	The format for the rectification request by the data subject should be specified i.e. if it should be in writing, in a form to be prescribed by the data controller or processor. Where the data controller or data processor has reasonable doubts about the identity of the individual making the request for deletion, correction or rectification of data, they should be able to request additional information to enable them to confirm identity. There should also be provisions to allow the controller/processor to delay the request until the identity of the individual is confirmed.
10.	Notification of breach of security on personal data	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, shall— (a) notify the Data Commissioner; and (b) subject to subsection (3), communicate to the data subject, unless the identity of the data subject cannot be established. (2) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller within the prescribed period.	The Bill should define the specific period within which a breach should be notified to the Data Commissioner. The Bill should define the prescribed period within which a data processor should notify the data controller.

		(3) The data controller may delay notification referred under subsection (1) (b), for purposes of prevention, detection or investigation of offences by the concerned public body. (4) The notification to the data subject shall be in writing and shall be communicated in the prescribed manner.	The period within which the notification may be delayed should be defined. It should be specified whether a notification may be transmitted via electronic communication.
11.	Rules as to data centres and servers	S. 44 (3) Cross border processing of Sensitive Personal Data is prohibited	We propose that the exceptions provided under S. 45 (1) should be extended to the processing of sensitive personal data.
12.	Cross Border Transfer	S. 45. (1) (b) The data subject has given explicit consent to the proposed transfer, after having been informed	We propose the adoption of the following text "…
13.	General principle of transfer of data	S.46 –Trans-border data transfer is permitted where the data controller or data processor has inter-alia given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data.	There is need for the Bill to define a benchmarked standard rather than utilise a subjective test to assess "appropriate safeguards" for the purpose of trans-border data transfers.
14.	Codes, Guidelines and Certification	S. 60. (1) The Data Commissioner may, for the purpose of this Act— (a) issue Guidelines or Codes of Practice for the data controllers, data processors and data protection officers; and (b) offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with this Act; (2) A certification issued under this section shall not alter the responsibility of the data controller or data processor for compliance with this Act.	We are of the view that this section should be deleted as it should be an industry-led process. The role of the Data Commissioner should be to facilitate and encourage this process. It may therefore be prescribed in the Policy.

		(3) The Cabinet Secretary may prescribe regulations for to govern the certification program	
15.	Regulations	S. 61 (d) The Cabinet Secretary may make Regulations for the better carrying into effect the provisions of this Act to provide for…the levying of fees and taking of charges	We propose that the implementation of this Act be funded by the National Treasury and that provisions on fees and charges be deleted.
16.	Transitional Provisions	N/A	We propose a detailed section that will provide for implementation of this Bill in a phased approach (as envisioned in the Policy). This will include what needs to come into force immediately and what will require later implementation after the institutional framework has been established.
17.	Second Schedule	Consequential Amendments	S. 84D of The Kenya Information and Communications Act should be removed since an intermediary does not have control over the data processing and ought not to be its liability.