GSMA Nairobi
Second Floor
Delta Corner Annex
Waiyaki Way
P O Box 45651-00100
Nairobi
Kenya
Tel: +254 709073000
gsma.com/mea

3rd October 2018

Chairperson
Taskforce on Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya.
Communication Authority of Kenya
P.O. Box 14448 00800
NAIROBI

Distinguished Chairperson,

RE: COMMENTS ON THE PROPOSED PRIVACY AND DATA PROTECTION POLICY AND BILL, 2018

On behalf of the GSMA and our members, I would like to congratulate the Government of Kenya on putting together a multi-stakeholder taskforce for the development of the privacy and data protection policy and bill. We are thankful and hopeful that this inclusive approach, to which one of our members is associated as a representative of the private sector, will equip Kenya with a robust and progressive framework to unleash further growth potential of the national digital ecosystem while providing a high level of protection to citizen and consumers for their personal data. These draft policy and bill could become an example of good practices for other African administrations which don't yet enjoy an overarching data privacy framework.

In response to the invitation for comments on the proposed Privacy and Data Protection Policy and Bill, the GSMA is pleased to submit for your kind consideration our feedback detailed below.

Our high-level comments focus on general consideration on how the current formulation would position the Kenyan framework within the broad spectrum of worldwide privacy policies and on a few more specific issues that the GSMA hopes could be reviewed based on alternative approaches or terminologies to enable a better balance between citizen and consumer protection and a striving data economy.

We make these submissions in good faith with the intention of contributing constructively towards the success of the development of the Privacy and Data Protection Policy and Bill in Kenya. We thank you for the opportunity to give our feedback to the Taskforce, and we assure you of our highest regard.

We remain at your disposal for any additional information on the attached comments. We would be happy to present to the task force our position and any of our research if these can help informing the finalisation of the draft policy and bill.

Yours faithfully,

Akinwale Goodluck
Head of Sub Saharan Africa
Email: agoodluck@gsma.com
Mobile: +254 798 485 214

About GSMA

The GSMA is the global mobile industry association with a membership of more than 750 mobile operators and more than 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.

GSMA Position Paper on the draft Data Protection and Privacy Bill 2018

The GSMA proposes the following changes to the draft Data Protection and Privacy Bill 2018:

1. **s. 27 - Lawful Processing of personal data.**

   Proposal:

   Maintain the current proposal.

   Rationale:

   The legal grounds for lawful processing of personal data established by the taskforce provide a sound and robust base guided by legitimate interests, including statistical research and further processing for compatible processes in line with international best practices. This gives solid foundation for protection with the necessary flexibility.

2. **s. 4 (1) (b)(ii) - Territorial**

   Scope Proposal:

   Remove the reference to equipment, and perhaps focus on processing of personal data that pertains to individuals in Kenya, carried out by foreign companies in Kenya.

   Rationale:

   Within the global privacy policy today the discussion focusses a lot on potential impact in terms of extra territorial effects and we acknowledge that this was a point of discussion by the taskforce. We have noted that the proposal uses the kind of pre-GDPR terminology of 'using equipment'. It is tempting to think that the current GDPR scope is too extraterritorial so it is good to avoid replicating it here, but on the other hand, if the trigger is 'use of equipment' then EU personal data that goes to Kenya will be subject to both EU and Kenyan rules which could cause confusion. There is therefore the risk of extraterritorial reach of applicability of any national privacy legislation.

3. **s.4 (2) (a) -**

   Scope Proposal:

   The rules should apply to all sectors both private and public.

   Rationale:

   If the goal is to enable digital transformation in Kenya, then individuals need to trust in the digital ecosystem that is growing around them. In order for them to trust in the digital ecosystem, they need to be provided with a consistent level of protection regardless of what technology they are using or what sector they are engaging with.

4. **s. 15 – 19 - Registration of Data controllers and data**

   processors Proposal:

   - The law should incorporate accountability mechanisms in lieu of stricter registration processes and should introduce lighter registration obligations.

   Rationale

   Accountability mechanisms will encourage organisations to adopt good practices by demanding that they should be able to demonstrate compliance either through the adoption of effective programmes or by making available certifications or codes of conduct.

   An approach more geared towards ex-post interventions by an administration with solid investigative powers will contribute better to its journey towards greater empowerment and quicker progress on the path towards building internal capacity, rather than a very detailed and administrative registration process.

   It is key that principles used to guide the law-making process are as broad based and general as possible in order to apply to the widest set of stakeholders and situations, avoiding the creation of derogatory regimes and the management of a long list of special cases.

5. **s. 23(1) - Data subject**

rights Proposals:

a) The right to be informed of the use to which the personal data is to be put – **Agreeable.**

b) The right of the data subject to access their personal data in custody of data controller or data processor – **Agreeable, but will require more detail with regard to limits and exceptions.**

c) Object to the collection or processing of all or part of their personal data – **Agreeable, but will also require limits specifically if related to legal and regulatory requirements.**

d) Correction of false or misleading data – **Agreeable. Propose timelines for processors and controllers.**

e) Deletion of false or misleading data about them – **Agreeable. Stipulate timelines for such requests.**

Rationale:

The data subject rights as highlighted in the Bill are good however there needs to be detail to define limits of and exceptions to the rights. These should also take into consideration matters of public interest, as well as requirements for legal and regulatory compliance.

6. **s. 28 - Conditions for consent**

Proposal:

Make the conditions for obtaining and withdrawal of consent clearer.

Rationale:

There are many different standards and contexts for consent. While the law should not be too prescriptive, a degree of certainty is needed regarding what is actually required of data controllers. Some of this can be provided in regulatory guidance, but

a basic standard (unambiguous, explicit, or express, etc.) should be stipulated in the law. An overly strict standard such as 'explicit' should be avoided as this is too cumbersome both for data controllers and data subjects. Additionally, clarity on the forms in which withdrawal can be effected will be critical.

7. **s. 29(3) - Processing of personal data relating to a**

   child Proposal:

   - Remove data controller as the guardian for the child.
   - Include definition of guardian that will include other relevant parties that are capable of operating objectively.

   Rationale:

   We welcome the fact that personal data of minors need to be addressed. We support the idea of appointing a guardian however the terminology data controller may bring confusion. Data controller may not be a suitable guardian, and therefore this needs to be reconsidered.

8. **s.34 - Right to data portability**

   Proposal:

   s.34 (1) Limit the data under this right to that which is identifiable. This will allow processors to apply mechanisms such as anonymization, and pseudonymisation so as to ensure that they are still maintaining the commercial aspect of the data.

   s. 34(5) – Limit the free requests to one, following which processors should be allowed to charge a reasonable fee.

   Rationale:

   Regarding the new right of data portability, further consideration should be given to the rationale behind such a rule. In the EU when the new right was introduced in GDPR, it was not entirely clear whether the policy objectives were about competition, consumer protection or data privacy. If the rule is to be included, there needs to be more clarification on what data is in scope. Data relating to an individual that is

generated by data controllers in the course of providing services, for example, should not be in scope by default as this could be commercially sensitive whereas the interests of consumers may be served by allowing them to port user generated content and account information.

9. **s 38 - Notification of breach of security on personal**

   data Proposal:

   Provide clarity on the timelines for reporting.

   S.38(6) – data breach reporting should always be mandatory, even where appropriate security measures are in place.

   Rationale:

   We welcome that the draft follows international trends imposing mandatory notification of security breaches subject to reasonable thresholds. The rationale behind reporting, is ensuring the data subject maintains control over their specific data. Therefore, the security measures of the data processor need not be taken into consideration.

10. **– Offences and Administrative Measures**

    Proposal:

    - Provide powers for the Authority to impose adequate administrative measures to deal with infringements of the laws well.
    - Recognise that in some cases, a breach may warrant a warning or reprimand from the Regulator, rather than an administrative fine or criminal liability.
    - Imposition of administrative measures should take into account seriousness of the infringement, including the nature, gravity and duration of the infringement, actions taken to mitigate damage caused by the infringement, whether any previous infringement have occurred and the level of safeguards the controller or processor has implemented throughout the organisation to demonstrate compliance. Other administrative measures should include actions such as cease and desist orders prior to imposition of administrative

fines. Administrative penalties should be a last resort after other civil measures have failed to take effect.

- Restrict criminal liability to the kind of activity referred to in s58 (unauthorised disclosure, access, sale, etc.) and removing criminal liability for general infringements of the law as is currently envisaged under sections 16(3), 16(7), 27(4), 42 and 52(3).

Rationale:

Criminal liability and imprisonment should be reserved for a much higher level of infringement as an ultimate last result and it is proposed that should be reconsidered. In some cases, even an administrative fine may be disproportionate, and a warning or reprimand may be more appropriate. Allowing a range of regulatory actions depending on the severity of the breach may encourage a more open dialogue with data controllers about how they can best mitigate privacy risks.

11. s 44 - Rule as to data centres and servers

Proposal:

The requirement to store a local copy of all personal data in Kenya, to prohibit transfer of 'critical' and 'sensitive' personal data altogether should be removed.

Rationale:

Data localization creates challenges in terms of reciprocity and lost opportunities for stimulating the data-driven economy in Kenya hence the need for clear definition and limited scope of application. Please see our reports including, Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers, Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows - How ASEAN and APEC can Protect Data and Drive Innovation, and Safety, Privacy and Security across the mobile ecosystem.

12. **s45, 46 Conditions for s45, 46**

Proposal:

The data controller should be able to demonstrate safeguards, but should not have to submit anything to the Data Commissioner in each case or in advance – only after the event.

We make these submissions in good faith with the intention of contributing constructively towards the success of the development of the Privacy and Data Protection Policy and Bill in Kenya. We thank you for the opportunity to give our feedback to the Taskforce, and we assure you of our highest regard.

GSMA