Principal Secretary, ICT & Innovation
Ministry of Information, Technology and Communication
Teleposta Towers
P.O Box 30025-00100,
Nairobi.

01-Oct-2018

Dear Sir,

RE: **COMMENTS AND SUGGESTIONS ON THE PROPOSED DATA PROTECTION BILL 2018**

Following your notice inviting the public to submit their comments on the proposed data protection bill and data protection policy 2018, I hereby send in my contributions for your consideration.

On **application,** personal data should also include any copies held in all the devices under the care of the data controller / processor e.g. personal data in test, development or non-production systems. The scope MUST apply to this type of data too not just data in production systems.

On **Categories of sensitive personal data,** there needs to be clarity on guidance on what is anticipated as sensitive data. The EU GDPR has some use cases which can be adopted.

On **duration of a registration certificate**, three years seems quite a long time given the dynamism of the technologies used to capture, store and process data. Unless the Office of Data Commissioner will have mechanisms to review on a periodic basis the level of compliance, this period needs to be reduced to an annual requirement.

On ***Complaints to the Data Commissioner,*** the provisions should give a guideline on process of making a complaint and the key considerations to validate a complaint.

On **Codes, guidelines and certification**, the issuance of certification should be visible to the data subjects either on the sources of data capture used by the data controllers or an information portal / query platform. This would give credence to a data controller's level of compliance with guidance on privacy.

On **rights of the data subject**, it is important to add that the data subject has a right to verify that a data controller / processor is registered and certified by the Data Commissioner to collect such kind of data.

On **conditions on consent,** it is important to clarify the implications of a data subject withdrawing consent. The data controller / data processor must surrender all data in their custody to the data subject.

On **automated individual decision making,** it would be useful to clarify on the sensitive categories of personal data e.g. disability, gender, religion etc.

On **limitation to retention of personal data,** it would be useful to clarify how long is long and provide a ceiling of the longest that data can be kept, for example a period not exceeding X years. Data Controllers / Processors need to take responsibility for the data, including complying with provisions for limited storage, to avoid unnecessarily holding data that is no longer needed under the guise of "reasonably necessary".

On **Investigation of Complaints,** it would be important to provide guidance on the key considerations of breach and the severity of penalty. The EU GDPR has guidelines on criteria e.g nature of infringement, intention, mitigation, etc. this is important to eliminate ambiguity during investigations.

I do trust that my contribution will be useful in providing a robust protection law for the citizen in accordance with our constitution.

Kind Regards,

Peter Muya,

ICT Consultant