Microsoft East Africa Ltd
P.O Box 64736-00620
The Oval Building
8th Floor, Ring Road, Westlands
Nairobi, Kenya

Tel: +254 -20-286-8000
Fax: +254-20-272-2999
www.microsoft.com/africa

18th September 2018

TO

JEROME OCHIENG
PRINCIPAL SECRETARY, ICT AND INNOVATION
MINISTRY OF INFORMATION AND COMMUNICATION
TELEPOSTA TOWERS
P.O. BOX 30025 – 00100
NAIROBI

MICROSOFT COMMENTS TO THE DRAFT KENYA DATA PROTECTION BILL 2018

Microsoft welcomes the opportunity to provide the Government of Kenya with its position on the best approach to the proposed data protection law.

We believe that an appropriate legal framework for data protection is the foundation on which data-driven innovation and entrepreneurship will continue to flourish in Kenya while at the same time respecting individual rights to privacy and data protection contributing to the respect for citizens human rights and fundamental freedoms as enshrined in Section 31 of the Constitution of Kenya 2012.

Included below are a few of our core recommendations to the proposed wording of the Bill as well as a a summary of the core tenets of global data protection law that we believe would provide the best foundation for Kenyan laws, regulations, policies, and guidelines on data protection. Implementing these practices will instill a level of trust in the local data protection legal regime that is necessary to propel trade, economic growth and job creation in Kenya.

Section A: Clause specific comments to the draft Bill

1. **Definitions:**

   "Encryption" means the process of transforming data into coded form;

Comment: Propose deletion as encryption methods may differ and are consistently evolving. Or revise to reflect: "Encryption" means the process of rendering information unreadable by unauthorized persons.

"Identifiable Natural Person" means a person who can be

identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

Comment: Collapse this under definition of data subject or under definition of personal data. Multiply definitions denoting similar content tend to lead to confusion.

2. Objects and Principles (Clause 3 and 4 – page 7-9)

Application 4. (1) This Actapplies to the processing of personal data —

(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means, providedthat when the recorded personal datais processed by non-automated means, it forms a whole or part of a filing system;

(b) to a data controller or data processor who –

(i) is ordinarily resident in the Kenya and processes personal data whilein Kenya; or

(ii) a legal entity duly incorporated or Registered in Kenyabut uses equipment in the Kenya for processing personal data, other than for the purpose of transit through Kenya;

(c) by a public body or a private body.

Comment: Microsoft supports having one data protection law applicable to all types of entities that process personal data. That said, propose simplification of this clause to avoid ambiguity of when the act applies:

"This Act applies to the processing of personal data of data subjects in Kenya, by making use of automated or non-automated means which form part of a filing system or are intended to form a part of a filing system, by

i) a natural or legal person;
ii) private or public entity

regardless of whether that person or entity is residing in Kenya or abroad.

(2) This Act shall not apply to –

(a) theexchange of information between Government departments and public sector agencies where such exchange is required on a need-to-know basis; or

Comment: Separate rules for public sector entities can have a place in the law. However, data protection rules that apply to the public sector should include meaningful restrictions on data processing to demonstrate that Kenyan law provides essentially equivalent protection to data protection laws in other regions to facilitate the free flow of data across borders.

Appropriate restrictions on data processing by the public sector are also important for fostering the trust of foreign data subjects whose data may be accessed by the Kenyan government.

3. **Registration of Data Controllers and Data Processors (Clause 16 – 20 Page 15 – 17)**

PART III— REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Comment: Consider practicality of registration process, cost and administrative burden of maintaining a registration process and similarly for conducting periodic audits of data controllers and data processors systems. It is likely better to require data controllers and/or processors to do periodic reporting and require third party audits of systems where necessary.

4. **Protection of Personal Data (Clause 23, 24 and 26 – Page 18 – 20)**

PART IV–PROTECTION OF PERSONAL DATA

23. (1) The following principles are applicable for the protection of personal data –

(a) the right to privacy of a data subject shall be safeguarded in processing personal data;

(b) personal data shall be processed for a lawful and explicitly defined purpose and shall not, without consent of the data subject, be processed in a manner incompatible with the intended purpose;

Comment: Microsoft aligns with the position that consent is an important ground for processing data, and the requirements for obtaining consent should be strong. However, consent should not be the only basis for processing data. The "legitimate interest" legal ground for processing, which is incorporated into many global privacy laws, is vital for enabling companies to collect data that is necessary to support, deliver and improve a variety of services for the benefit of the data subject, controller or society.

Propose revision to 23 (b) to reflect:

"Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes."

(f) where personal data is held by a third party, the data may only be released to another person with the consent of the data subject;

Comment: Consider revision to allow for release to another third person "with consent of the data subject or in according to a lawful Court Order issued in compliance with the local laws and regulations of the country where the Data is stored."

(g) personal data shall not be transferred outside Kenya, unless there is adequate proof that the recipient country has adequate data protection laws;

Comment: Propose revision to avoid double negative:
“Personal data may be transferred outside of Kenya subject to data controller and data processor having proof that the recipient country has adequate data protection laws to ensure the level of protection of data subjects guaranteed under this Act is not undermined.

Rights of a Data Subject.

24. (1) Subject to the provisions of this Act and any other written law, a data subject has the following rights with respect to personal data—

No.31 of 2016.

(a) right to access and enquire on the details of processing personal data, in accordance with the Access to Information Act, 2016 and the prescribed procedure;

(b) right to information on the manner in which personal data shall be processed including the category of the data, the intended recipients or the period within which the data shall be stored;

(c) right to rectification;

(d) right to be forgotten or right to erasure;

(e) right to be informed and object on profiling of personal data based on automated decision making:

Comment: Propose revision of 24(1)(b) to reflect the right to know what data is collected about the data subject and the purpose for which data is processed, including:

- The categories of personal information collected,
- The categories, if any, of third parties with whom personal information has been shared.
- Where and how data is used and for what purposes.

Collection of personal data.

26. (1)A data controller shall, subject to subsection (2), collect personal data directly from the data subject.

(2) Despite subsection (1), a data controller shall not be required to collect personal data directly from a data subject where—

(a) the data is contained in a public record;
(b) the data subject has deliberately made the data public;
(c) the data subject or a competent person, where the data subject is a child, has consented to the collection from another source;
(d) the data subject has consented to the collection from another source;
(e) the collection from another source would not prejudice the interests of the data subject;

(f) collection of data from another source is necessary-
(i) for the prevention, detection, investigation, prosecution and punishment of crime;
(ii) for the enforcement of a law which imposes a pecuniary penalty;
(iii) for the protection of the interests of the data subject or another person;
(iv) to comply with an obligation imposed by law; or
(v) in the interest of national security; or
(g) compliance is not reasonably practical.

Comment: Propose deletion of 26(1) and (2) as this may cause ambiguity. It is sufficiently noted under 26(3) that data should only be collected, stored or used for specified purposes, using lawful means and in a manner that does not hinder the personal affairs of the data subject. Alternatively delete Section 26(2)(a) to (e) and include provisions (f)(i) to (v) under Clause 4(2) which outlines instances where requirements under the Act shall not apply. This is consistent with data protection practices in other countries where right to privacy is balanced with ensuring public safety and security are protected.

5. **Processing of personal data (Clause 28(5) – page 22)**

(5) With respect to foreign data subjects, the data controller shall ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction of that data subject, where personal data originating from that jurisdiction is sent to the Kenya for processing.

Comment: The complexity of requiring multiple compliance standards based on nationality of data subject, could create minefield for data controllers or data processors to comply with. That said principle of adequacy as already introduced within the Act should ensure that when processing personal information of foreign data subjects adequate protections are provided for as outlined in This Act. Propose deletion of this sub-clause.

6. **Data Portability (Clause 34(5) – page 25)**

(5) A data controller shall comply with the subject portability requests, free of charge and within one month, however, the data controller may extend the period for a further two months where requests are complex or numerous.

Comment: The requirement to have data portability is understood, that said this should not be at the cost of the data controller nor should there be a prescribed timeline when this should be concluded. Propose revision to reflect the following:

"A data controller shall comply with the subject portability requests within a reasonable time period."

7. **Security safeguards for personal data (Clause 37) – Page 23)**

(2) To give effect to subsection (1), the data controller shall take reasonable measures to—

Comment: Propose revision as follows:

"To give effect to subsection (1), the data controller shall consider measures including but not limited to the following"

(3) In determining the appropriate security measures referred to in subsection (1), in particular, where the processing involves the transmission of data over an information and communication network, a controller shall have regard to the –

(a) state of technological development available;

(b) cost of implementing any of the security measures;

(c) special risks that exist in the processing of the data; and

(d) nature of the data being processed.

Comment: Propose revision as follows:

"In determining the appropriate security measures referred to in subsection (2), in particular where the processing involves the transmission of data over…"

(4) Where a data controller is using the services of a data processor –

(a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection (1); and

(b) the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

Comment: Propose revision to (4)(b) as follows:

"the data controller and the data processor shall enter into a written contract which shall specify the conditions for processing of the personal data including the data processors obligations with regards to security measures to be undertaken to comply with the obligations under Clause 37(1)."

8. Sensitive Data (Clause 40 and 43 – page 29 - 30)

PART V— SENSITIVE PERSONAL DATA

Restrictions to processing of sensitive Personal Data.

40. (1) A data controller or data processor shall not process sensitive personal data.

(2) The provisions of subsection (1) shall not apply where processing of personal data is —

(a) the data subject consents to the processing;

(b) required under national or international law;

(c) carried out for statistical or research purposes;

(d) publicly available; or

(e) the processing is on a matter which is of public interest;

(2) Any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable, on conviction, to a fine not exceeding ten million shillings, or to imprisonment for a period not exceeding five years, or to both.

Comment: Laws should not broadly restrict the processing of sensitive personal data. Rather, the level of restriction on the processing of personal data should correspond to the context in which the data is processed.

- In general, processing of sensitive information should be allowed where appropriate safeguards for the security and privacy of the information are in place, where the data subject is adequately informed about the collection and use of the sensitive data prior to sharing the data and has legitimate options to refrain from sharing the data, or where adequate de-identification, subject to sufficient technical and organizational measures preventing reidentification, is employed.

Data subject's health

43A data controller or data processor may process data relating to a data subject's health where a data controller or data processor is –

(a) a medical institution or social service institution processing data for purposes of treatment and care of the data subject;

(b) an insurance company or a medical scheme processing data for purposes of entering into or performing an insurance contract;

(c) a school processing the data for purposes of providing special support for students in connection with their health;

(d) a public or private body acting under a lawful duty to manage the welfare of a data subject; or

(e) an administrative body, pension fund, or employer processing data for purposes of implementation of the law relating to the health of the data subject.

Comment: Instead of focusing on the type of entity or institution which may create barrier for entry to market for innovators, propose the following revision:

"Processing of data related to a data subject's health is permissible for the purposes of:

(a) treatment and care of the data subject;
(b) performance of a contract relating to provision of treatment or care of the data subject
(c) lawful means required to manage the welfare of the data subject
(d) implementation of the law relating to the health of the data subject."

9. Transfer of Personal Data outside of Kenya (Clause 46 – page 31)

General principle of transfer of data.

46. (1) A data controller or data processor may transfer personal data to another country where –

(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;

(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards;

(c) the transfer is necessary for –

(i) the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the

Comment: Clarification required to make clear that it is "either" "or" i.e.: proof of adequacy or explicit consent or transfer is necessary etc.

Microsoft

<u>Section B : Other general comments to the draft Bill in line with international best practice</u>

Subject Matter Scope

1. Consumer Privacy Rights

- GDPR establishes important new privacy rights that are relevant globally. Microsoft has extended the rights at the heart of GDPR to all of our consumer customers worldwide. Kenyan law should grant consumers data subject rights that are at the heart of GDPR.

- The consumer data subject rights that should be required in Kenya are:

    - To know what data is collected about the data subject and the purpose for which data is processed, including:
        - The categories of personal information collected,
        - The categories, if any, of third parties with whom personal information has been shared.
        - Where and how data is used and for what purposes.

    - To receive an electronic copy of the personal data collected.

    - To request rectification of inaccurate personal data.
        - The preference should be to enable rectification through a secure, automated system that enables data subjects to correct their personal data directly. However, the rectification obligation should also be able to be met through manual processes where necessary.

    - To delete personal data, subject to certain exceptions.
        - Companies should be permitted to retain data if there are "overriding legitimate grounds for the processing." This exception should include the ability to retain data for important security purposes.
        - Companies should also be permitted to retain data when necessary for compliance with a legal obligation, such as laws mandating certain retention periods.

- Data subject rights should only be granted subject to thorough authentication and verification of the consumer's identity.

2. Responsibility – Controller/Processor Distinction

- It is important to maintain a distinction in responsibility between a data controller, which determines the means and purposes of processing data, and a data processor, which processes the data on behalf of another organization.

- A data controller should be primarily responsible for meeting privacy obligations and for providing redress to individuals. So long as a data processor merely processes data on behalf of a data controller, the processor's responsibility should be to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations.

- Liability should be allocated among organizations that process data according to their agreement, or barring an agreement, then according to demonstrated fault giving rise to the liability.

3. Consent and Other Grounds for Processing

- Consent
    - Consent is an important ground for processing data, and the requirements for obtaining consent should be strong.
    - Consent should not be the only basis for processing data. GDPR includes strict standards for ensuring consent where consent is necessary, but also identifies other equal legal grounds of processing, including processing that is necessary for legitimate interests, performance of a contract, compliance with a legal obligation, or tasks carried out in the public interest.
    - Providing notice and obtaining consent at the point of data collection is at times either impractical or unnecessary. Individuals can be interrupted and overwhelmed if constantly presented with privacy choices and requests to collect data.
- Legitimate Interest
    - The "legitimate interest" legal ground for processing, which is incorporated into many global privacy laws, is vital for enabling companies to collect data that is necessary to support, deliver and improve a variety of services for the benefit of the data subject, controller or society.
    - GDPR includes a provision allowing processing based on legitimate interest, which must be demonstrated through a rigorous, documented analysis of privacy risks and mitigations that confirms the controller's legitimate interest (the lawful benefit that the controller or third parties derive) in processing personal data outweighs the impact of the processing on the interests and rights of the data subject (i.e. the residual risks).
    - Kenyan law should adopt the concept of legitimate interest to legitimize processing previously collected data, particularly when there are purposes for processing the data that may not have been knowable at the time of collection, so long as such processing is subject to rigorous documentation of the privacy risks and mitigations.

- For example, the legitimate interest ground for processing data in the AI context should be applicable where a company engages in robust pseudonymization of data, puts in place accountability measures such as commitments not to reidentify the relevant data, conducts a thorough, documented assessment of the impacts and risks associated with the data processing, and documents and implements safeguards to minimize the identified impacts and risks.

4. Sensitive Data

- It makes sense to provide additional protections to sensitive personal data that present a high level of privacy risks.
- The definition of "sensitive personal data" should be aligned to modern norms to include data revealing personal financial information, racial or ethnic origin, political opinions, or religious beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation.

- Laws should not broadly restrict the processing of sensitive personal data. Rather, the level of restriction on the processing of personal data should correspond to the context in which the data is processed.

    - In general, processing of sensitive information should be allowed where appropriate safeguards for the security and privacy of the information are in place, where the data subject is adequately informed about the collection and use of the sensitive data prior to sharing the data and has legitimate options to refrain from sharing the data, or where adequate de-identification, subject to sufficient technical and organizational measures preventing reidentification, is employed.

5. De-Identification

- Lawmakers should promote the use of data that has been subject to de-identification techniques that either eliminate or reasonably reduce the ability to connect data with a specific individual.

    - An all-or-nothing approach that mandates full and irreversible de-identification is a very difficult (some argue impossible) standard to confirm and achieve.

    - There are benefits from reasonably de-identifying data that outweigh the risks. Reasonable de-identification enables broader development and use of cloud and artificial intelligence, while effectively protecting people's privacy at the same time. It also has positive implications for science, as researchers will be able to more easily replicate and advance other people's work.

- Data that is reasonably de-identified, coupled with a commitment to not reidentify the data, should not be subject to data subject rights.

- The commitment to not reidentify the data should apply both to the controller of the data, and to any other entity to whom the controller provides the data.

6. Territorial Scope

- Countries should not seek overly broad extraterritorial application of data restrictions. Data protection laws that claim broad extraterritorial application are disproportionate in the online environment, create challenges for compliance and enforcement, work against global norms, and risk hampering innovation and growth for both domestic industry and companies with global operations. Sweeping application of such laws may create a reciprocity effect which may impede the ability of domestic companies to operate internationally as well as restrict the level of business which could get sent to Kenya for data processing or analysis.
- The international community recognizes that each country is fully entitled to regulate information within its borders, but generally not outside its borders.
- National security is a legitimate motivation for accessing personal data and maintaining cross-Fundamental Rights report on surveillance law in Europe, "international intelligence cooperation is an absolute must in light of today's myriad threats" – and this requires cross-border transfer, as intelligence services may need specialist resources or access that they do not have locally. However, compliance with international agreements, such as Mutual Legal Assistance Treaties (MLATs) is critical when data that raises specific privacy risks is to be shared with law enforcement organizations in third countries. Microsoft supports efforts to improve upon current bilateral and multilateral government data sharing agreements.

7. Cross-Border Data Transfer

- Kenya's data protection law should facilitate intercompany and cross-border data flows that are protected through appropriate technical and legal measures and not otherwise prescribe the location of data.
- Often well-intentioned, cross-border transfer restrictions and data localization measures can be difficult to implement, damaging to the economy, and unable to address the primary privacy concerns associated with data processing. A more effective approach is to adopt regulation that is interoperable with global standards or contracts that protect personal data regardless of its location. Such an approach can also help to improve resiliency and security and make data processing services more efficient by reducing latency. It will then be incumbent on data processing companies to make sure that the personal data that they process is managed according to local law, regardless of the location to which it is transferred.

- Examples of international data transfer standards and contracts that Kenya should consider leveraging include:

- Certification to Industry Codes of Conduct: Industry codes of conduct, developed through open, multi-stakeholder processes, are an effective mechanism for allowing companies to show their compliance, including through certifications to international standards such as ISO/IEC 27001/27018. Recognizing these programs across borders, such that a given mechanism can be used in multiple markets, will provide consistency for regulators and customers evaluating companies' compliance, while not being overly bureaucratic. It is an effective way of addressing privacy and security concerns associated with emerging technologies and rapidly evolving business models.

- Accountability: We favor approaches aligned with the OECD "Accountability Principle" that allow data to be transferred across borders if the data controller remains accountable for protecting the data regardless of its geographic location.

- Data Transfer Agreements Consistent with EU Standard Contractual Clauses: If a contractual model for legitimizing international transfers is to be pursued, then data transfer agreements that require protections consistent with the EU Standard Contractual Clauses should be recognized as an acceptable mechanism for maintaining accountability and legitimizing cross-border transfers.

- Bilateral or Multilateral Frameworks: Leveraging existing bilateral and multilateral frameworks would enable companies to use established principles and mechanisms to protect the privacy and security of personal data as it moves across borders. The EU-U.S. Privacy Shield, for example, offers a bilateral cross-border data transfer framework that could be a model for other jurisdictions.

8. Security Breach Notification

- Notices should not be required in cases where the breach does not threaten real harm to the individuals involved; a regime that requires notification even for harmless breaches threatens to engender "notification fatigue" and lead individuals to ignore notices.

- Over-notification could also potentially make it more difficult for the relevant regulator to focus resources and attention when material breaches occur. The EU General Data Protection Regulation addresses this issue by excluding from notification requirements breaches that are unlikely to result in a risk to the rights and freedoms of individuals.

- It takes time to evaluate the nature and scope of a breach and whether a breach is likely to cause harm to data subjects. While it is important to notify impacted consumers in a timely manner, it is more important for the notice to present the facts of the breach fully and accurately. Also, a short turnaround will ultimately shift focus to reporting and administrative burdens rather than breach mitigation. The law should avoid a prescriptive timeframe, and we instead suggest notification be made without undue delay.

The EU General Data Protection Regulation and many U.S. state laws, for instance, allow for notification to be delayed for justifiable reasons.

9. Children

- Special consent requirements should apply at least for children under the age of 13. This aligns with U.S. practice. The EU General Data Protection Regulation requires parental consent for children under 16, but allows EU Member States to revise this requirement to children under the age of 13. A requirement to seek parental consent for processing of children's data is reasonable in most cases, although the cut-off age of 16 may be too high if it cuts off young adults from the Internet.

- Parental consent should not be required in all circumstances. For example, where responsible parties are under a legal obligation to process children's data they should not be required to seek parental consent.

- It should be permissible to process children's data when doing so is necessary to comply with a legal obligation or to guard the health or ensure the physical integrity of the child.

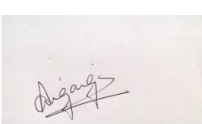
10. Tech Neutrality

- Technology-specific language can get outdated quickly. Laws should be as technology neutral as possible. The benefits of cloud and artificial intelligence can only be fully realized once cloud infrastructure reaches a critical level of scale with global reach.

- As an example, Cloud computing enables rapid analysis of large of amounts of data and pattern recognition. These capabilities, when paired with human creativity, empathy, emotion, physicality, and insight, serve to augment human abilities and experiences and move society forward. Indeed, data analytics, machine learning, and artificial intelligence made possible by cloud computing are helping organizations in manufacturing, education, healthcare, and many other sectors understand complex systems, improve efficiency, reduce costs, solve difficult problems, and deliver new capabilities.

- Kenya is currently at the forefront in the region on exploring use of new emerging technologies such as cloud, AI, blockchain to name but a few to rapidly transform the economy – national legislation needs to be conducive and forward thinking enough to embrace the rapid evolution of technology.

Compiled by:



ANGELA NG'ANGA
CORPORATE AFFAIRS LEAD
MIDDLE EAST AND AFRICA EMERGING MARKETS (MCC)

CC. CHAIRPERSON
TASKFORCE ON DEVELOPMENT OF THE POLICY AND REGULAORY FRAMEWORK
FOR PRIVACY AND DATA PROTECTIONIN KENYA
COMMUNICATIONS AUTHORITY OF KENYA
P.O. BOX 14448 00800
NAIROBI