U.S. CHAMBER OF COMMERCE

USAFRICA BUSINESS CENTER

September 19, 2018

Mr. Jerome Ochieng
Principal Secretary, ICT &Innovation
Ministry of Information Technology and Communication
Government of the Republic of Kenya

Mercy Wanjau
Chairperson
Taskforce on Privacy & Data Protection
Government of the Republic of Kenya

Dear Mr. Ochieng and Ms. Wanjau,

On behalf of the U.S. Chamber of Commerce and the Chamber's U.S.-Africa Business Center, we respectfully submit our comments on the recently released Data Protection Bill and Data Privacy Policy documents. The U.S. Chamber is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. Housed within the Chamber, the U.S.-Africa Business Center is the only institution of its kind representing the interests of both U.S. and African business communities.

As vocal advocates for increased bilateral trade between the U.S. and Kenya, and regional trade across the African continent, we appreciate the opportunity to provide feedback and stand ready to assist the Kenyan government to develop sound data protection policies.

We view Kenya as an important IT hub for the African region, and the home of the 'Silicon Savanah.' To continue to attract foreign direct investment, we recommend a flexible, risk-based privacy regime that recognizes differences among industries in their use of data, enables legitimate business uses of personal data, empowers consumers to make informed choices, and enables cross-border data flows.

We encourage the Kenyan government to leverage the data privacy principles created by the Organization for Economic Co-operation and Development and Asia Pacific Economic Cooperation. These international best practices prioritize the importance of data flows to ensure the Kenyan economy and consumers remain connected digitally to the rest of the world.

It is vital that the Kenyan government ensure a coherent, streamlined set of rules and establish clear authorities that minimize complexity. We have therefore outlined the attached recommendations to the current draft bill in an effort to ensure Kenya benefits from the full range of beneficial data uses in the modern information age.

Sincerely,

Scott Eisner
Senior Vice President
U.S.-Africa Business Center

Sean Heather
Vice President
Center for Global Regulatory Cooperation

Procedure and Application

First, we seek clarity on the interaction between the Draft Data Protection Bill 2018 and Privacy and the outlined Data Protection Policy 2018 that are currently under request for comment. Any policy and legislative instruments that are not aligned will create confusion for both individuals and companies operating in the Republic of Kenya. It would be helpful to better understand the vision for how these instruments are intended to operate in practice. Moreover, it would appear that the Policy covers all data, of which personal data is a subset, making the extent of the obligations unclear and potentially overly broad.

The following comments reflect specific recommendations.

Specific Comments and Recommendations on Kenya Data Protection and Privacy 2018

We recognize that both of these documents draw from the European Union's General Data Protection (GDPR). The policy document in particular appears to act as a summary of these concepts. However, as it lacks any amendments and recitals similar to what is in GDPR that would put these provisions into context, it risks being near impossible to implement. For example, requiring the regulator to be notified about all data breaches without any threshold will likely overwhelm the regulator. Even with the limited threshold that the EU has put into place, many European data protection authorities are experiencing with GDPR now in force.

Section 5: Principles of Data Protection

Within the principles of data protection, processing restrictions should not exclude the ability to process data in the legitimate interests of the data controller, provided there is no unreasonable and manifest detriment to the individual. The GDPR provides for such safeguards. For example, a firm may choose to outsource its data storage to a cloud provider or outsource its payroll to a third party. Data subjects should not have the right to prevent these types of processing and transfer by the data controller, which is in the data controller's legitimate interests, provided appropriate safeguards are applied.

In addition, "journalism" should be included in Section 5.2 in addition to the list of further processing purposes that are allowed under the purpose limitation, as this is a consistent practice in privacy legislation globally.

Section 7: Legal Grounds for Processing

In regards to Section 7.4 on third party processing, it is not practicable or possible for an individual to be made aware of every third party who processes their personal data. For example,

a bank account could involve processing by the bank, its affiliates, suppliers who provide technical support, the telecommunications companies who host the lines, and other parties. Further, this information does not enhance or better protect an individual's personal data. Instead, the privacy policy should be focused on ensuring that data controllers follow data protection obligations to all suppliers and third parties with access to personal data rather than having to make data subjects aware of all third party processing.

Section 8: Obligations for Data Processing

As previously referenced, the current language around when a data breach should be reported is too broad and will result in over-reporting. Data breaches that do not involve any material risk or harm to the individual should not need to be reported to the regulator. The purpose of breach reporting is to ensure firms are complying with obligations to protect data, and to ensure individuals can make informed decisions about data controllers and take steps to protect their data as needed. If data is encrypted or at no risk of misuse, it is unclear why a notification needs to be made, and what is the benefit.

Section 8.2.8 outlines an obligation to nominate a data protection officer (DPO). As exists in GDPR, a threshold should be put in place outlining when a company should be obliged to nominate a DPO. Otherwise, small and medium sized enterprises (SMEs) without sufficient resources or funding to support this role will not be able to fulfill this obligation. Given the wide-scale presence of SMEs in the tech entrepreneurship ecosystem in Kenya, this regulation could significantly hamper these entrepreneurs from establishing and scaling their businesses.

Appendix A: Definitions of Key Terms

The definition of anonymization is practically impossible to comply with in a quickly evolving technological age. With enough time, financial resources and technology, all data is potentially re-identifiable. The definition should be amended so that it is closer to similar definitions in other laws whereby data is "not readily or economically likely to be re-identified."

Specific Comments and Recommendations on Data Protection Bill 2018

Sensitive Data

We support creating different categories of data in order to facilitate a risk-based approach to data protection. We suggest further clarifications on language qualifying that genetic or biometric data should expressly be linked to an individual or medical record in order to encourage innovation and continued medical research. Great medical advancements are currently occurring through the use of genetic data, which is often anonymized or thoroughly randomized and aggregated so as to make the individuals virtually un-identifiable.

In order to encourage innovation and avoid unnecessary costs to businesses, we suggest indicating that for sensitive data, legitimate interest be recognized as a means of processing. Sections 40 and 47 should be broadened to encompass processing for the purposes of complying with, or assisting other persons to comply with, a requirement which involves a person taking steps to establish whether another person has (i) committed an unlawful act, or (ii) been involved in dishonesty, malpractice or other seriously improper conduct. In addition, the data controller should not be obliged to obtain the consent of the data subject for this type of processing.

In addition, the conditions to permit processing are currently closed-ended rather than being based on a flexible assessment of risks and safeguards. A context-driven, risk-based approach to consent has proven successful worldwide. It may also be beneficial to allow for legitimate interest-based processing of sensitive data in contexts where obtaining consent would be impossible or impracticable. For example, the 'legitimate interest' provision provided for sensitive data does not appear to apply to corporations. A balancing test and safeguards would be more effective at addressing the sensitive nature of the data in contexts such as these.

Section 44(3) prohibits cross-border processing of sensitive personal data, which would make it impossible to pursue legal claims, investigate alleged offences, devise global diversity strategies, provision of health care etc. Safeguards should apply to sensitive personal data, but not prohibitions on transfer.

Anonymized Data

We welcome language in the draft recognizing anonymization as an important tool for data protection. We believe that anonymization helps decrease the risk to individuals and should be exempt from the draft. We suggest adding clarification that personal data only includes data or processed data sets related to reasonably identifiable individuals and does not include de-identified or anonymized data. This removes uncertainty and allows for responsible entities to conduct risk assessments for realistic scenarios, in particular benefitting small businesses that have fewer resources. Narrowing the language will serve to encourage greater use of anonymization.

In addition, we would suggest adding language to the definition of pseudonymization in the draft to clarify that pseudonymization is another useful technical mechanism to safeguard data, and should not only be considered as a risk. The definition in the current text treats pseudonymized data as personally identifiable information (PII) without qualification.

Section 22: Principles of Data Protection

We recommend changes to or the deletion of two principles: (g) only released to a third party only with the consent of the data subject; and (h) not transferred outside Kenya, unless there is adequate proof of adequate data protection laws by the recipient country.

We suggest an amendment to (g) that allows for the creation of the principle of lawful processing under which the processing of data in accordance with any of the legal bases identified in Article 27. Data transfers to third parties should be allowed to occur as long as the third party ensures that adequate measures are in place for the protection of personal information. This is consistent with international best practice. The EU's 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). The current approach is a concern from an operational perspective, and will debilitate Kenya's ability to do business globally. We propose that Kenya follow the GDPR's model, which adopts a "legitimate interest" approach.

Further, concepts of country-level "adequacy" are often problematic, inconsistent, and deter innovation. It is unclear within the draft what constitutes "proof" of privacy adequacy of a third country, and how a private organization is expected to obtain or assess what constitutes "proof." It also undermines the concept of model clauses or consent or other safeguards as established means of protecting personal data when made available outside the country of origin.

By limiting data transfers to the countries in a list, Kenya will find it more difficult to interact with the global digital economy and will deprive its citizens of the products and services they seek. Instead, we recommend a more flexible approach that allows the transfer of personal data outside the territory of the Republic of Kenya, unless it results in the demonstrable and defined harm to the data subject.

Section 27: Lawful Processing of Personal Data

We welcome language in the draft that acknowledges a variety of mechanisms for processing, in particular legitimate interest as a legal basis for processing data. Legitimate interest protects individual data by requiring that a risk-based assessment is made in each instance.

At the same time, this language would be more useful if the text were to drop references to non-consent based processing as an "exceptional circumstance." Different mechanisms for processing data, including mechanisms based on legitimate interests, should be presented as equivalent bases for ensuring legality, as they are in the GDPR, not as "exceptional circumstances."

As exists in privacy regulation around the world, we suggest adding journalism as a basis for processing in section 27(1)(viii) and 35(1)(d).

Section 30: Restrictions on Processing

Restrictions on processing should be subject to processing in the public interest. Specifically, Section 30(1)(a) should not require firms to cease processing data of individuals while a request is being contested. This may allow bad actors to manipulate credit reference agencies and risk intelligence databases by requiring their data to be suspended during a time where they can effectively "play" the system and apply for positions/products/services, which they would otherwise be disqualified from or be assessed as a high risk if the information about them had been readily available.

Section 33: Restrictions on Processing

Firms should be allowed to contact individuals to assess whether they wish to receive marketing materials, otherwise data controllers end up in a "chicken and egg" situation where they can't contact individuals to ask their preferences. In addition, this provision should be prohibiting firms from analyzing data and assessing preferences of clients, which is different from direct marketing.

Section 34: Right to Data Portability

As GDPR is demonstrating, a right to data portability is technically challenging for many companies. Given that individual's already have the right to access and rectify their data under the current draft, it is likely unnecessary for that data to be provided in a machine-readable format. Further, given technical challenges and varying amounts of data involved, the time period to reply to such requests should not be limited to one month but rather focus on a timely response consistent with how difficult the request may be.

Section 35: Limitation to retention of personal data

Firms should be permitted to retain data in accordance with their obligations and policies, including those of their parent companies and home regulators or laws.

Section 36: Right of Rectification and Erasure

We have concerns with references in the draft to a "right to be forgotten" or "right to erasure." Hosting platforms already give users the ability to delete or erase information that the user has posted or uploaded to the platform. In those contexts, giving users a "right to erasure" with respect to content that they have uploaded would not meaningfully change the options that users already have. However, there is a risk that a "right to be forgotten" or a "right to erasure" could be interpreted too broadly, creating significant operational burdens and legal uncertainty for small companies and startups in Kenya and elsewhere.

This proposed right opens up a number of complex legal and operational issues around the ability of a user to censor online content, such as how to balance the interests of users and

publishers; how to balance one user's privacy interests with another user's free expression and journalistic interests; and, how to account for the broader public's right to know the truth and have access to accurate historical records. In many cases, individual content hosts and publishers are not well-placed to adjudicate conflicts between these rights.

Additionally, while some large companies may be able to pull together legal and technological resources to operationalize these rights, this compliance obligation would drastically reduce the possibility for new platforms, search engines, and internet services -- including local services -- to enter the Kenyan market.

Section 45: International Transfers

While adequacy is an optional tool, in order for Kenya to better integrate and benefit from the global digital economy, it should use a combination of various transfer mechanisms.

It is not clear how the balance between the legitimate interests of the data controller and the rights and interests of the data subject as set out in section 45(1)(vi) will be assessed, and this is critical for all firms operating via the cloud or beyond the immediate borders of Kenya in any way. Given the evolving landscape of privacy laws in Africa, and that those countries with privacy laws are fewer than those without such laws, it is unclear how even local transfers and processing will continue to take place effectively.

Recognizing these mechanisms allows the seamless flow of data and positions Kenya as an active player in the global digital economy. We recommend changing the language so that the international transfer of personal data is allowed in the following cases:

- to countries that provide a level of personal data protection at least equal to that of this Law;
- where the transfer is necessary for international judicial cooperation between public intelligence and investigative authorities, in accordance with international law;
- when the transfer is necessary for the protection of the life or physical safety of the data subject or a third party;
- when the competent authority authorizes the transfer;
- when the transfer results from a commitment made in an international cooperation agreement;
- when the transfer is necessary for the execution of a public policy or of a legal public attribution, being publicized under art. 24; or
- when the data subject has provided consent for the transfer, with prior specific information on the international character of the transaction, having been informed of the risks involved.

- when the controller proves that the transfer is based on standard contractual clauses approved by the competent authority or recognized under internationally accepted rules or codes of conduct;
- where the controller proves that it holds seals or certificates issued by certification bodies qualified and approved by the competent authority.

Kenya should look to the APEC Cross-Border Privacy Rules (CBPR) system, which recognizes more legitimate mechanisms such as privacy marks and organizational codes of conduct that are certified by a competent authority or third party. Kenya could allow recognized certification bodies to authorize such mechanisms, such as the Accountability Agents in the APEC CBPR system to avoid approval bottlenecks within this competent body. Mexico is also taking steps in this direction and has recently put in place a self-regulatory mechanism in order to be compatible with the CBPR system and allow for even more secure and reliable data flows. Even though Kenya is a non-APEC economy, it can attract investment and interest from companies within the APEC CBPR system by designating CBPRs as a valid mechanism to transfer data and potentially even develop a compatible standard.

Including widely-accepted concepts of "model contracts and clauses", "standard contractual clauses", and "global corporate standards" or "global corporate rules" (known in Europe as "Binding Corporate Rules" or "BCRs.") will also help Kenya seamlessly integrate into the global digital economy. Such clauses should also allow a company or group of companies engaged in joint economic activity to use the same structure for international data transfers in order to ease the cost and time of doing business. These clauses typically include minimum conditions such as detailing the structure of the company, information about the data and transfer process, and how to apply general data protection principles.

Another option could be by simply establishing that the international data transfers may occur freely subject to the principles established in this law. The need for prior approval from competent authorities for international data transfer is a heavy burden and is not adequate in the context of a global economy where international data transfers are necessary and part of companies' daily business operations. One example is to create exemptions for intra-group data transfers. Both Mexico and Colombia utilized these exemptions. International data transfers are responsible for the rise of new businesses around the world and the digital economy. The Internet and its capacity to enable the free flow of information is a major boost to economic trade and new business models operating exclusively online. If there is a need for a formal authorization from the competent authority for international data transfers, day-to-day business operations as well as the development, growth, and spread of innovation and new technologies, such as the Internet of Things (IoT), would probably be negatively impacted.

We believe that concepts of country-level "adequacy" are often problematic, inconsistent, and deter innovation. By limiting data transfers to the countries in a list, Kenya will find it more difficult to interact with the global digital economy and will deprive its citizens of the products

and services they seek. It is essential that all determinations are made in a transparent and timely manner. We also suggest creating guidelines requiring the collection of stakeholder input in order to create a fully informed assessment.

Part II: Office of the Data Commissioner (Data Protection Authority)

We welcome the text's reference to creating a data protection authority to oversee the implementation of the regulation. When developing the Data Commissioner, we encourage the government to show leadership in terms of international best practices regarding the creation of a data protection authority.

The implementation of the bill will be dependent on a competent, well-funded independent functioning authority. Complying with new requirements will take both extensive monetary and technical resources and companies will require adequate lead time to ensure proper implementation. Therefore, we suggest the final Draft Bill specify that any effective date not occur until after the creation or designation of a fully functioning competent authority. Time will be needed for the technical and operational changes needed for compliance. We also suggest minimum time allocations for implementation of any future requirements developed by the competent authority. We stress the importance of appropriate phase-in periods for compliance with any additional requirements as determined by the competent body.

The U.S. Chamber of Commerce has published a report, Seeking Solutions: Attributes of Effective Data Protection Authorities, which outlines seven key traits that effective DPAs share and offers examples of how DPAs have incorporated these traits. The seven traits are:

1. Promote Education and Awareness
2. Seek Feedback
3. Offer Guidance and Assistance
4. Act Judiciously
5. Act Transparently
6. Strive for Coordination and Cooperation
7. Be Business and Technology-Savvy

Part VIII: Enforcement Provisions

The Commissioner will play a vital role in making sure that the regulation is implemented and enforced. Therefore, the law should not go into effect until after this authority is in place and has had time to issue guidance around the various responsibilities it is delegated within the law.

While the GDPR put in place a two-year implementation timeline, EU Member States already had functioning data protection authorities that were able to quickly start issuing guidance around implementation. Even still, some EU Member State governments did not have

the necessary guidelines and regulatory updates in place by the time GDPR was in force. As countries begin to establish privacy regimes based on GDPR, such as this regulation proposes, we strongly caution against including an implementation period that does not take into consideration the extra time it will take to set up a brand new data protection authority. Other governments that did not take into consideration the need for a data protection authority to be in place before enforcement, have experienced delays in implementation and confusion from stakeholders around how to comply with the law.

Rather than putting an implementation period into the law, we encourage the government to include language recognizing the need to have a Data Commissioner in place before implementation and enforcement of the law. Further, until this time, companies should be able to continue to collect, share, process and transfer data under their current procedures.

Section 59: Offences

We strongly recommend that any language around imprisonment as a penalty is struck from the regulation. GDPR penalties do not include imprisonment. In regards to civil penalties, the proposed regulation should be consistent with the privacy laws of other countries. In addition, there should be more clarity regarding the civil penalty imposed, as the regulation does not specify what currency the fine would be in, nor does it provide a range.

***

The U.S. Chamber of Commerce and the Chamber's U.S.-Africa Business Center appreciate the opportunity to offer our views on the creation of a data privacy regime in the Republic of Kenya. If you have further questions about this submission please contact Brionne Dawson (BDawson@USChamber.com) and Kara Sutton (KSutton@USChamber.com).