UBER

**UBER B.V.**
VIJZELSTRAAT 68
1017 HL AMSTERDAM
CHAMBER OF COMMERCE: 56317441

2 October 2018

Mr Jerome Ochieng, Esq
Principal Secretary for ICT and Innovation
Ministry of information, Communications and Technology
Teleposta Towers
Nairobi

By email

Dear Sir

**Submission on the Data Protection Bill, 2018 (the "Proposed Law")**

We refer to the above matter and wish to express our gratitude for the opportunity to submit our feedback on the Proposed Law. We also welcome development efforts by the Government of Kenya in this field and as a technology company, are grateful to be included as part of the industry's stakeholders.

We have had a chance to review the Proposed Law and we believe it is a positive step to better protect Kenyan's personal data. There are few areas where we are of the view that the Proposed Law could provide better clarity to both individuals and companies operating in the Republic of Kenya on their respective commitments to protecting data privacy. Our comments below utilize our local knowledge of Kenya's priorities in this space, as well as global experience advising on and complying with newly enacted privacy law abroad.
Having said the above, please find our comments below:

**Section 15: Registration of data controllers and data processors**

We recommend to have removed the requirement for data controllers and processors to register with the Data Commissioner. Legislative developments across the globe have been moving to accountability models where the companies need to be able to demonstrate that they can comply with data protection laws. This has been a shift from the requirement of prior notification or registration with the competent authorities, which is an administrative burden for both the companies and the authorities that have to maintain those registries, without a practical effect on the protection of personal data. Having to register the processing activities with an authority is burdensome and poses barriers to innovation, which would require every detail of an operation to be communicated to the authority. It would also require the Data Commissioner to maintain resources to enable companies to submit this information, to issue certificates, and to keep it up-to-date. As an alternative, an accountability principle could provide adequate means for companies to demonstrate compliance to the Data Commissioner.

**Section 33: Processing for direct marketing**

Similar to other foreign laws, companies would benefit from the possibility to process data for direct marketing based on legitimate interests, including for the sending of electronic marketing messages. Thus, we recommend using this legal basis in the Proposed Law, allowing companies to inform their own customers of new or updated products and services, as there is in this case a prior relationship with the customer and an expectation of communications. A safeguard for this position would be to allow the customers to opt-out of direct marketing at any time.

**Section 44: Rule as to data centres and servers**

The Proposed Law would require companies to store data in Kenya. This would result in substantial costs for companies operating in the country. These costs would, for example, relate to the need to maintain additional servers, and to the increase of processing and additional measures required to maintain data accurate, secure, and up-to-date. Local companies that rely on international storage and processing, especially startups and SMEs, would likely incur in substantial costs to operate. It may also prevent certain companies from offering services to Kenyan consumers, leaving them with less choice.

This requirement can create a gap between the availability of hosting services and the required security capabilities regarding the risks posed by the processing of personal data, leaving companies without a compliant option to operate.

The Proposed Law prohibits the cross-border processing of sensitive data. A limitation such as this would effectively prevent certain services that rely on sensitive data from being possible, for example, related to health and safety. Instead, companies should be able to demonstrate that they have in place adequate measures, such as contractual mechanisms, to ensure that data is protected in cross-border activities.

**Obligations of processors (multiple Sections across the Proposed Law)**

Many of the provisions in the Proposed Law use the EU GDPR as a guide, including the concepts of a data “controller” and “processor.” Making this distinction helps define the varied obligations between controllers and processors; notably, the GDPR uses degree of control over the data in question as an important factor in determining these obligations. The controller determines the purposes and means for the processing whereas the processor acts on behalf of the former.

However, while the Proposed Law makes that distinction only conceptually. In practice, it applies the same obligations to both data controllers and data processors.

Effectively, this would mean that data processors that act on behalf of controllers would be responsible for complying with obligations which would be very difficult, if not impossible, given the role that they have in the processing. This would lead to problematic scenarios such as the ones exemplified below:

- A data processor in Kenya enabling emailing services to a data controller would need to make sure that an email sent on behalf of the data controller is accurate;

- A data processor in Kenya providing data hosting or storage services would need to ensure that any personal data stored on behalf of the data controller is processed with a legal basis, such as consent of the data subject.

The proposed application of these obligations to the data processors goes far beyond the scope of the GDPR, obviates the need for a distinction between controller and processor, and makes compliance for processors exceedingly difficult. It will make future compliance very difficult for companies acting as data processors. Therefore, and in line with other data protection laws, we recommend the following obligations to be applicable solely to data controllers: Sections 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 44, and 46.

All of these obligations would remain part of the data controller's responsibility, which in turn should ensure that the data processors they use provide the appropriate safeguards.

If you have any questions on our submission, please do not hesitate to reach out the undersigned using the contacts provided.

Yours faithfully
For and on behalf of
Uber

Cezanne Maherali
Head of Policy, Uber East Africa
cezanne@uber.com