An update on the Data Protection Bill 2019: a step forward for Kenya.

Kenya is making good headway towards the process of enacting its first primary piece of data protection legislation.

The revised Data Protection Bill 2019 (the **Bill**) was gazetted on 5 July 2019 and represents a positive step forward after much to-and-fro. Please click here for some background.

Conditions for cross-border transfers

One of the major concerns with the previous texts of the draft legislation was the requirement for the local storage of personal information. The sentiment was that these restrictions were counter-productive to emerging technologies (in particular cloud computing) and would result in unnecessary hindrances to the ever-evolving technological landscape that is shaping the everyday lives of Kenyans.

The Bill permits the cross-border transfer of personal data subject to certain conditions being met. These include adequacy of appropriate safeguards, consent of the data subject, the transfer being necessary to perform a contract, implementation of pre-contractual measures, or for any matter of public interest.

However, the Bill introduces a very broad carve-out allowing the Cabinet Secretary to prescribe that a certain type of processing should only be effected through a server or data centre located in Kenya. This would be permissible 'based on strategic interests …or … protection of revenue'. No further details are given and this, together with the fact that the Cabinet Secretary can exercise these discretionary powers at any time, creates uncertainty, in our view.

It would have been a welcome clarification had the authors of the Bill set out the specific circumstances or factors that the Cabinet Secretary will take into account before imposing the requirement that certain data be processed in Kenya. Equally, we would hope that the Cabinet Secretary, when introducing any such cross-border restrictions, would at the same time also allow for certain exemptions or exclusions to be applicable in appropriate circumstances. This, we believe, would give some comfort to international entities doing business or otherwise offering services in Kenya.

Appropriate safeguards required but not spelt out

While cross-border transfers of personal data are not restricted as long as one of the conditions for transfer is met, there is a proviso: personal data can be transferred outside of Kenya only if the Data Commissioner has been provided with proof on the 'appropriate safeguards with respect to the security and protection of personal data'. What is disappointing is the absence of additional criteria for determining what 'appropriate safeguards' are. Again, this gives wide discretion to the Data Commissioner to provide its approval according to its own criteria.

Sensitive personal data will be afforded even more stringent protection. The Bill does not expressly prohibit the cross-border transfer of sensitive personal data, but makes it subject to certain conditions and safeguards, for example the prior consent of the data subject must be obtained. Note that sensitive personal data includes data revealing an individual's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, sex or sexual orientation. A person's political opinion is no longer classified as sensitive personal data.

The new Bill has retained the Office of the Data Commissioner, which will keep a register of all data controllers and data processors over whom the Bill may have jurisdiction. Given the requirement for registration, it is important to note that a data controller or data processor is one of the following:

(i) an entity established or ordinarily resident in Kenya that processes personal data while in Kenya; OR

(ii) an entity that is not ordinarily established or ordinarily resident in Kenya but processes personal data of data subjects in Kenya.

Registration is valid for a period of three years and may be renewed, but there is no indication as to what fees will be charged. Importantly, there appears to be no distinction between small and medium sized enterprises (SMEs) and larger enterprises, which arguably have more human and financial resources to spend on compliance matters. The absence of any thresholds for registration with the Data Commissioner may result in potential bureaucratic difficulties for SMEs striving to comply, thus creating further barriers to entry.

In terms of the penalties that may be imposed for contravening the provisions of the Bill, the maximum amount for an infringement of the Bill by a person is up to KES 5 000 000. In the case of an undertaking, it is up to 2% of annual turnover (whichever is the higher). We have requested clarification, as it is not clear whether the Bill will adopt the penalty regime introduced in certain other jurisdictions and extend the calculation of an undertaking's annual turnover to mean global turnover. Where no specific penalty has been provided for, a person may be liable to a fine not exceeding KES 3 000 0000 or to imprisonment not exceeding two years, or both.

Despite the remaining uncertainties, the Bill does represent a significant and commendable step forward. The rights of data subjects will certainly have increased protection and we look forward to moving ahead with the implementation of this Bill.

Please do not hesitate to contact John Syekei or Ariana Issaias if you have questions or queries relating to this article.