Kenya - Privacy and Data Protection Bill 2018

Amazon Web Services ("AWS") welcomes the opportunity afforded the company to comment on the Privacy and Data Protection Bill ("The Bill"). The Bill provides an opportunity for a close consideration of the cloud as a next generation Internet and Communications infrastructure and platform and for the construction of a regulatory framework that would guide the provision of data services on the cloud.

Our principle concern is that there would seem to be evidence of a lack of understanding of how services are provided in the cloud; further, role confusion and conflation of parties identified as key role players in the Bill within Kenya and role confusion of parties identified as the providers of services in locations external to Kenya. In addition the obligations and responsibilities placed on the identified key role players in the Bill –"Data subjects"; "Data processors" and "Data controllers" as well those of external "third parties" seem misplaced in the cloud computing context. In turn the obligations placed on a "Data Subject" are a matter of concern in a context of a data subject's capacity to fulfil obligations placed on them. There is accordingly scope to reconsider these roles and to properly locate the roles, obligations and responsibilities of all parties.

The starting point would have to be to address the conceptualization of cloud computing. The cloud, in the AWS context, provides a platform on which a hyperscale computing platform and its services are made available to customers. The AWS Global Infrastructure is a global server-based hardware platform from which core AWS platform services in the form of Compute, Storage, Database and Networking services are provided. This global infrastructure is made available from a growing infrastructure base, currently 36 disparate "Regions" from which a fully redundant and fail-safe cloud platform and its services are provided from locations across the world. It is from these regions that cloud services are made available to customers by AWS from edge locations optimized for size of market and access to time sensitive data.

In making cloud services available, AWS works in accordance with a Shared Responsibility model with respect to the provision and access of cloud services. AWS, as the cloud platform provider is responsible for the security of the cloud platform and in turn the customer is responsible for the security in the cloud, like identity and access management; threat protection, vulnerability management and operations. The is responsible for other items like encryption and data integrity; authentication of server-side data and networking traffic protection.

The Bill does not address cloud services in this manner. A cloud service provider is not accorded an identity in the data regulation framework the Bill sets out. With respect to the categorization of service providers, there is an insufficient differentiation of the role of a putative cloud services provider from a "data processor" and/or "data controller". There is in effect a confusion and conflation of their roles. A "data processor" and/or "data controller" would ordinarily be a user of a cloud services platform. In the ordinary course a "data processor" and or "data controller" would not make use of the services of a party either in Kenya or in another country providing services which are identical to the one that the "data processor" and/or "data controller" would themselves provide. The Bill however

accords a role identical to that of a “data processor” to an external “third party” providing what would seem to be equivalent services to those provided by a “data processor and/or “data controller” but under the authority of a data controller or processor. A close reading would suggest that the role accorded the external “third party” is a role expected of an external cloud services provider. There is in turn a confusion and conflation of roles as between a “data processor” and “data controller”, two identified categories of service provider in the Bill. In many instances the same statutory obligations apply to both parties. It is accordingly difficult in many instances to differentiate one from the other. Many of the statutory obligations placed on a “data processor” apply equally to a “data controller” and could be provided by either one of them. Role clarification as to the ascribed roles of “data processor” and “data controller” beyond the definition provided in the Bill would accordingly be welcome.

T

Data Controllers and Data Processors

In terms of Section 15 of the Bill “subject to exemption, no person shall act as a data controller or processor unless registered with the Data Commissioner”. To this end, in terms of Section 16 of the Bill, “all persons who intend to act as either data controllers of processors shall apply in the prescribed form” detailing - personal data to be processed; a statement as to whether they are likely to hold categories of sensitive data as defined; description of the data to be processed; description of the recipient to whom the data controller or processor intends to disclose personal data.

As outlined above, we have identified a number of concerns with the conceptualization of “data controllers” and/or “data processors”.

Although what constitutes a “data controller” or “data processor” is contained in the Part 1 of the Bill-

a “data controller” being defined as “a natural or legal person, public authority, agency or other body, which alone or jointly with others, determines the purposes and means of processing of personal data” and a “data processor” being defined “as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller”, the two terms are, as stated earlier, often conflated in the Bill. The possibility that the data controller and data processor may be one and the same person or legal entity is not addressed, there is in fact no prohibition in this regard and there is little to distinguish what applies to one the exclusion of the other or would apply to both in defined circumstances.

Section16 (2) provides that in an application to the Data Commissioner for registration, the applicant must provide:

(a) a description of the personal data to be processed by the data controller or data processor, and of the category of data subjects, and of the category of data subjects to which the personal data relates.

(d) a description of any recipient to whom the data controller or data processor intends or may intend to disclose the personal data.

Equally it is not clear given what is stated above why the obligation in Section 16 (e) for "the name, or a description, of any country to which the data controller intends or may wish, directly or indirectly, to transfer the personal data" should not apply equally to a data processor wishing to attend on the same process.

These concerns extend to provisions in the Bill dealing with the prevention of unauthorized access, processing and disclosure in the Bill; the obligation to correct inaccuracies in processed records; and the requirement for data processors and controllers to attend on processing in a secure manner; and to retain customer confidentiality (Section 22 (1)).

Although the Bill is crafted in line with the general principles that underpin robust data protection regulatory regimes like the European Union's General Data Protection Regulation ("GDPR") 2018, the Bill could be strengthened and brought into line with international best practice by ensuring that the provisions of the Bill that are at variance to best practice as identified, reflect such practice.

Data protection, the principal and over-riding concern of the Bill is addressed in a number of sections and in different contexts in the Bill.

In Section 16 (Part III Registration of Data Controllers and Data Processors) - requires a " description of the purpose for which personal data is to be processed" to be made known to the Data Commissioner (16 2 (d); a description of any recipient to whom the data controller or data processor intents or may intend to disclose personal data (16 (2)(d) ; the name, or a description of any country to which the proposed data controller intends or may wish, directly or indirectly to transfer the personal data of a data subject(16 (2) (e); a statement as to a representative for the purpose of this Act and details of such representative 16 (2) (f) ; a general description of the risk, safeguards, security, measures and mechanisms to ensure the protection of personal data. (Section 16 (2) (h)).

In turn Section 45(1) provides – (a) the data controller or processor may transfer personal data to another country where they have 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 such transfer such as the absence of appropriate security safeguards (c) transfer must be held necessary for -
(i) performance of the contract between data subject and data controller or data processor or for implementation of pre-contractual measures taken at the data subject's request;
(ii) the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another person;
(iii) any matter in the public interest:
(iv) the establishment, exercise or defence of a legal claim;
(v) in or 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) the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of data subjects.

A number of these provisions are at variance with international best practice. As a general rule and regardless of context, personal data should only be made available to a third party, however that party is identified, by a data processor or data controller only with the informed consent of a data subject. This would be in line with the provisions of Section 22 (1) (Part IV – Principles and Obligations of Personal Data Protection) of the Bill which stipulates that "Every data controller or processor shall ensure that personal data is-

a) processed in accordance with the right of privacy of the data subject:
b) processed lawfully, fairly and in a transparent manner in relation to any data subject
c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
e) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal are erased and rectified without delay;
f) kept in a form which identifies the data subjects for no longer than is necessary for the purposes of which it is collected;
g) only release 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.

It should be noted in this context that reference is made in Sub Section 22 (1) (g) to the release of personal data to a "third party", defined in Part 1 as a "natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority, are authorized to process personal data;" As noted earlier a cloud services provider would never be authorized or assume the right to process the personal data of a data subject per the formulation outlined above. A cloud services provider is only in a position to provide the platform on which a duly authorized provider of data processing services, be it a data processor or data controller, as defined, would have the right to attend on the processing of personal data as he or she deems fit.

It should also be noted that Section 22 (1) (h) contains a prohibition on the transfer of personal data outside Kenya unless there is adequate proof of adequate data protection laws by the recipient country."

This provision, aside from a proposed minor reformulation as to make it read "…of adequate proof of adequate data protection in the recipient country" would be sufficient by most purposes.

However, in Clause 45 (1) (Part VI – Transfer of Personal Data Outside Kenya) additional constraints are imposed in the form of – in subclause 45 (1) (a) and (b)
-which requires that a data controller or processor must give "proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data" and the data subject to give "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".

The consent process outlined in Clause 45 (1) (b) the draft Bill is problematic. Aside from the fact that it places an unduly onerous burden on the data subject to provide "explicit consent" instance in which the cross-border processing of data is required by a data controller, it requires an assessment of data transfer risks by a data subject in circumstances where the data subject may not be in a position to conduct such an assessment. It would be preferable if provision was made for the prior general approval of cross border data processing by the data processor or data controller in the form of either signed or "ticked box" electronic consent by the data subject, subject to the explicit commitment to adherence by the data controller to generally applicable and accepted security controls on both the handling and the transfer of personal data as provided for in Section 22.

The standard of proof required for the transfer of personal data should be objective evidence that adequate measures, principally in the form of law, regulation and certification processes, are in place for the protection of personal data in a country other than Kenya where personal data processing takes place. It should sufficient for the data processor or data controller to provide such evidence and for there to be an expectation of reciprocity to govern the transfer and processing of personal data from countries other than Kenya which processed on Kenyan cloud services infrastructure.

This would be line with GDPR standards which require general consent and notification by data processors prior to data transfer to a jurisdiction where personal data processing takes other than the jurisdiction where such data is collected. In addition, that the country in which such processing takes has data protection laws in place that are deemed adequate, on an objective basis, for the protection of personal information. In all such instances it should be noted that it would be the Kenya data processor and/or data controller who would processing such data on a cloud platform made available for his/her use. The data processor or data controller's responsibility for making use of the cloud service platform in accordance with the laws governing the processing of personal data in Kenya would remain, particularly with respect to the requirements pertaining to the anonymization and/or pseudonymisation of data.

In practice this should allow for the transfer of personal data to a processing location in countries that have a level of personal data protection that is commensurate to the data protection laws found in Kenya.

The determination of what constitutes commensurate protection would ordinarily be data protection of the standard required for international judicial co-operation between countries, more specifically with respect to personal data transfer, standards that would be accepted or recognized under internationally applicable rules for the secure transfer of confidential private data. A data processor or data controller would have to provide evidence that they are certified in accordance with requisite standards applied by an international certification body. The data processor and/or data controller would have to attest to the fact that they qualified to attend on the secure cross border transfer of personal data and to hold and process such data in a secure manner in a country other than Kenya.

Equally, a cloud services provider whose platform is used for processing purposes by the data processor or controller would be expected to confirm that the infrastructure on which processing is undertaken by a data processor or controller meets the necessary certification requirements for the use of the cloud services platform for the processing of personal data. Ideally such standards should be applicable irrespective where the cloud services platform is itself located.

It would accordingly be preferable to amend the provisions of Sections 16 (g) and 46 (1) of the Bill to enable this and in so doing make the existence of objective standards-based safeguards, as outlined above, the sine qua non of the cross-border transfer of data. This would obviate the need for the provisions of Section 46 (1) and 45 (1) (b) of the Bill.

In line with the position set out above, the provisions of Section 3 (b) (Part I - Preliminary) which speak to a "restriction to further processing" should preferably be amended to reflect a "restriction on illegal and/or unwarranted processing" as all processing would be undertaken by a data controller and/or data controller in accordance with the provisions of applicable law, irrespective of where such processing takes place.

It should be noted that in terms of Section 46 (1) "The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests". Further that the Data Commissioner "may in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined".

As outlined above, it would be preferable for a data processor or controller, where a data processor or controller wish to transfer data to another country, to provide evidence of its adherence to objective, internationally benchmarked and reviewed cyber security standards that the data processor or data controller applies, to demonstrate "the effectiveness of security standards" rather the subjective test outlined in Section 46 (1) above.
Equally, should the cross-border transfer of personal data be mandated by "compelling legal interests", rather than a casuistic and subjective assessment of what constitutes "compelling legal interests" it would be preferable if the term "compelling legal interest" were to be defined. The test of demonstrable and defined benefit to the data subject should be one determined either in terms of cost, efficacy, convenience and availability or the unavailability of equivalent services. This would make for ascertainable objective standards.

Enforcement and Penalties
Section 51 grants the Data Commissioner explicit enforcement powers – (a) to investigate the compliant or cause it to be investigated by an investigating officer. The Data Commissioner may for the purposes of an investigation, order any person to (a) attend at a specified place and time and to be orally examined in respect of a compliant; (b) produce such book, document, record or article as may be required with respect to the investigation (c) furnish a statement in writing made under oath or on affirmation.

In terms of 52 (2) the Data Commissioner's investigatory power to require access to any information stored in any mechanical or electronic device investigate or for such information to be made available.

Section 59 (1) in turn stipulates that "A person who commits an offence under this Act, for which no specific penalty is provided or who otherwise contravenes this Act, shall on conviction, is liable to a fine not exceeding five million or to an imprisonment term not exceeding five years or both".

Aside from the fact that a monetary penalty is not stipulated in Section 59 (1) it would be preferable if the Bill did not impose penal sanctions and left sanctions of this nature as matters to be adjudicated om by courts of law. In addition, ideally no penalties either financial or penalties should not be imposed until after a "lead in" period of preferably five years in which applicable law, regulations, infrastructure and processes are put into place by the Data Commissioner to manage data protection. Needless to say, this process should be accompanied by education and awareness campaigns directed at all affected parties.