12 September 2018

Kenya Data Protection Bill

Thank you for the opportunity to submit comments to the Kenyan Ministry of Information, Communications and Technology on its draft Policy and Regulatory Framework for Privacy and Data Protection.

It is welcome to see a draft Bill addressing a wide variety array of key protections that are essential for a modern, technology-neutral and forward-looking data protection law. The draft Bill is a good starting point for a law that will need to be appropriate for the data-driven economy and society, be capable of enabling both effective privacy protections and innovation, and ensure Kenya's economic competitiveness in the fourth industrial revolution.

As a general point, to ensure consistent compliance from global organisations that operate and/or process data in Kenya, the draft Bill should align itself as much as possible with existing global data privacy laws and standards, while at the same time building and improving upon existing models to devise more effective solutions to the challenges of the modern digital economy. Kenya can benefit from the experience of other parts of the world with regard to what aspects of their data protection regimes have worked well and which have not. As Kenya progresses this Bill it might be helpful to look not only to the EU General Data Protection Regulation (GDPR), but also to privacy regimes in other jurisdictions and regions (including the APEC region).

It is welcome to see the draft Bill establish a single and effective national data protection authority and include concepts such as data protection principles, grounds for processing personal data, the distinction between data controllers and data processors, transparency and individual rights. On the other hand, the draft Bill would benefit from some clarification and modification in certain areas, as outlined in more detail below.

The draft Bill does not though provide for a risk-based approach or the accountability principle for controllers, which is a much more effective way to ensure appropriate governance and protections than a system of approvals, checks and prescriptive obligations and restrictions.

It is not clear what the relationship is between the policy document and draft Bill, or how they are intended to work together. There are elements in the policy document that appear to belong in the draft Bill, or would be better served by being in the draft Bill. A single data protection document outlining the principles, rights and responsibilities provides legal clarity and certainty for both individuals and organisations, as well as enabling more effective enforcement by the data protection authority.

The comments and recommendations presented are intended to assist the drafters in progressing the Bill in a way that fully realises its promise, and are based on experience of data protection laws in practice in other jurisdictions both from the perspective of a practitioner making it work in businesses and as a regulator having to implement and enforce it.

It would be helpful to have a second round of consultation on a revised version of the draft Bill before its enactment.

Part 1, section 2: definitions

Sensitive data definition: includes 'personal preferences'.

This would seem to be a vague and subjective term and without further clarification could include, for example, my language preference on a website, the types of newsletters I wish to receive from a company, or the information on my supermarket loyalty card about the items I buy most often.
Due to the restrictions on processing sensitive data, including this term in the sensitive data definition undefined could have a significant impact on non-contentious and necessary data processing.

Cross-border processing definition
"Cross-border processing" means —
(a) processing of personal data by a data controller or data processor who is outside Kenya; or
(b) processing of personal data while outside Kenya but which substantially affects or is likely to substantially affect the data subject in Kenya;

This definition is confusing as both (a) and (b) include controllers and processors outside Kenya. It is not clear what (b) is trying to achieve that is not already achieved by (a). The wording looks similar to the EU's GDPR, but in GDPR the wording relates to the fact that an entity may have activities in multiple states across the European Union. This geographical set up is not applicable to Kenya.

As the definition relates to part 6 on transfers of data outside Kenya, and the only provision referencing this definition is at 44(3) prohibiting cross-border processing of sensitive data, it may be more effective and less confusing to refer instead to a transfer. In defining a transfer, it would be helpful to align with other data protection regimes who consider a transfer to be where personal data is sent to another country, or where there is remote access to in-country data from another country. The advantage of this definition is that the subsequent obligations on organisations who transfer data are on those who make the decision to send the data elsewhere (or allow remote access). The existing definition in the draft Bill would cause these obligations to fall on organisations who happen to be outside Kenya, rather than the organisation who made the decision to send the data there, and so who should have the responsibility to ensure compliance.

If (b) is retained, a clear definition of 'substantially affects' is needed.
The unclear definition also has a negative impact on the transfer rule at section 44(3), which prohibits any cross-border processing of sensitive data. This is commented on later in the section on transfers.

Part 1, section 4(1)(b)(ii): application
4 (1) This Act applies to the processing of personal data —
(b) to a data controller or data processor who:
(ii) [is] not established or ordinarily resident in Kenya, but uses equipment in the Kenya for processing personal data, other than for the purpose of transit through the country;

The EU changed this aspect of its law when it upgraded the 95/46 Directive to the GDPR due to the significant differences in interpretation of 'equipment' and the unintended negative impact that this has had over the years. To avoid the same mistakes the EU made, and the varying interpretations of the provision, it may be beneficial to amend section (ii) above as follows.

(ii) is not established or ordinarily resident in Kenya, but offers goods or services to data subjects in Kenya, or monitors their behaviour as far as their behaviour takes place in Kenya.

Part 1, section 4(2)(a): application
(2) This Act shall not apply to –
(a) the exchange of information between government departments and public sector agencies where such exchange is required on a need-to-know basis;

It is difficult to see why no governance or data stewardship requirements would be necessary for public sector data sharing, so a blanket exemption may not be the most appropriate way to both facilitate necessary sharing and protect individuals' personal data. Perhaps this provision could instead reference a framework for necessary and proportionate data sharing, the details of which could be left to the Data Commissioner.

Part 2, section 6(2): qualifications of the Commissioner
In this section there seems to be some missing text. The qualifications are listed as being "(a) and (b) or …", but there is no (c).

Part 3: registration
The provisions seem to be similar to those of the EU 95/46 Directive. Experience in the EU has shown that requiring companies to complete lengthy forms detailing processing activities has served little purpose and has instead become an administrative burden for both companies and the data protection authority. This is why the EU removed this requirement from GDPR and instead put the responsibility on the organisation to maintain appropriate internal records, that the data protection authority could request to see.

Before requiring any registration scheme it is important to articulate what purpose it is intended to serve. In the UK, there will continue to be a basic registration scheme, as the UK data protection authority is funded by fees imposed on organisations, so a registration scheme is needed to collect the fee. A basic scheme is also useful generally for a data protection authority to understand what kinds of organisations and data processing are taking place in its jurisdiction, so they can tailor advice and guidance accordingly. A basic register also provides necessary contact details for the organisation.

It may be worth reconsidering the detailed provisions in this section to avoid making the same mistakes as the EU.

Part 3, section 21: DPO
It would be worth considering adding safeguards for the DPO to this section, so that they are protected from being instructed by their employers to present a particular view, or to ignore activities that may not be compliant. It would also be helpful to make clear that the responsibility for compliance lies with the organisation, and that the DPO is there to provide advice and guidance, and cannot be held personally liable for an organisation's failings, in particular where they have not taken the advice of their DPO.

Part 4, section 22(g): principles
(g) only released to a third party only with the consent of the data subject;

Many organisations to carry out their business rely on outsourcing certain processes and activities to others. This would all be put in jeopardy with this principle that there cannot be any disclosure to a third party without consent. It is not clear what protections or controls this principle aims to achieve and what harm it is seeking to prevent. In other data protection regimes disclosures to third parties are considered a processing activity, which therefore has to have a lawful grounds. This could be consent, but it could also be any of the other grounds for processing, so the organisation can use the one that is most appropriate for the scenario.

Part 4, section 23(1)(e): rights
A data subject has a right to —
(d) correction of false or misleading data; and
(e) deletion of false or misleading data about them.

It is important to clarify in relation to these rights that it is in relation to personal data that is factually inaccurate that an individual is able to request correction or deletion. Without this clarification there is a significant risk that organisations will be forced to amend or delete valid opinions (such as in the medical profession) or information that the individual merely claims is false or misleading. Experience in the UK with credit reference agencies and the impact of inaccurate data on individuals has led to a situation where evidence of factually inaccurate data allows an individual to correct tor delete data. In addition, where there continues to be a dispute over what is factually correct, the individual is allowed to add a note to their file to set out their disagreement.

Part 4, section 25(2)(g): exemptions from direct collection
25 (1) A data controller or data processor shall collect personal data directly from the data subject.
(2) Despite subsection (1), personal data may be collected indirectly where:
(g) compliance is not reasonably practical.

This clause would seem to provide a blanket exemption from many aspects of the proposed law simply because an organisation decides compliance is not practical. It would seem odd to remove appropriate data governance obligations just because the information comes from a source other than the individual. In fact, it would seem logical to require additional governance obligations where data is collected from another source, given the increased risk that the data may be inaccurate or incomplete. The provision also assumes that all organisations have a direct relationship with an individual, which is not the case, especially for business-to-business products and services.

To achieve the aim of better protection of personal data for individuals, the same principles and governance obligations should apply, regardless of where the data has come from. Where the data has been collected from somewhere other than the individual, it is more important to ensure accuracy and to be able to provide information to the individual on where the data came from.

What is also missing from this provision is a recognition that organisations get data from other sources as a necessary part of delivering a product or service. For example, many organisations use credit reference agencies or other sources to verify identity, check credit and so on. There is no provision for this non-contentious and necessary data processing in the Bill.

Part 4, section 26(1): information to the individual
26 (1) A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject [about]—

(d) the intended recipient of the data;
(e) contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

Clauses (d) and (e) seem to overlap as they both reference other third parties who may receive personal data. This can be resolved by deleting the last part of (e) as follows. (e) contacts of the data controller or data processor;

Part 4, section 29: children
This section references the need for parental consent and age verification but there is no reference to the age at which an individual is considered to be a child, and / or when parental consent is necessary. These clarifications are essential to make this provision work and be enforceable. A sensible approach may be to align with the most common international practices of having the age threshold for a child as 13. This is the case in the US under COPPA, the recent Brazilian privacy law, and many EU Member States who have 13 as the age of digital consent as set out in article 8 of GDPR.

It is also worth noting that age verification may not be the most effective way to protect the child, given the risk of children feeling compelled to circumvent these measures. The mandate to use age verification could result in a perverse incentive that hinders the development of more effective privacy protections. A more effective approach could be to demand for in-context settings that are easily accessible and easy to use. The age-verification mechanism chosen should involve an assessment of the risk of the proposed processing and should not lead to excessive data processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are or are not a minor.

It is also important to avoid a system where every site or service, even those not intended for or attractive to children, must age-verify their users. Organisations that do not explicitly direct their services at children should not be required to implement age verification, and a risk-based test can be used to determine whether a service is directed at a child (such as whether it processes large volumes of children's data, and the intent of the organisation to target children). It is also worth noting the potentially onerous nature of implementing such solutions could lead businesses - out of caution - to choose to stop providing services to children or users suspected to be children under a specific age. This could exclude large parts of the internet from use by children - including valuable sources of information, learning, and communication.

The draft Bill should also recognise situations where children's data will be processed without age verification or parental consent where this processing is necessary to comply with a legal obligation, an order of a court or tribunal, or for prompt action, including the need to guard the health or ensure the physical integrity of the child.

In addition, blanket restrictions on online tracking in respect of children under section 29(4) could lead to a restricted ability to provide relevant information to the individual, especially in education tech and over-the-top (OTT) services. It could also prevent the provision of key services, such as fraud prevention in the banking sector, where organisations monitor and track savings accounts and financial activities to prevent and detect suspicious transactions.

Part 4, section 31: automated decision making

There has been significant debate in the EU over the equivalent provision in both the old and new law, as some data protection authorities have interpreted it as a right, and some have interpreted it as a prohibition. It is written in the draft Bill as a right, which is the right approach, but to function properly it also needs safeguards for the individual for when the right does not apply, so that individuals are not discriminated against and have some form of redress against automated decisions that negatively affect them. Examples of safeguards could be that in the scenarios in section 31(2)(a) and (c), the organisation must put in place appropriate safeguards and provide the ability for the individual to contest the decision and ask for human review.

Part 4, section 33: direct marketing

This provision is not clear whether consent is also required for B2B marketing, where an individual's' work details are used to send them marketing. Including B2B marketing would have a significant negative impact on many organisations and their ability to promote and grow their business activities by marketing to individuals in their professional capacity. It would be helpful to specify that B2B marketing is excluded and to add the general safeguard for everyone that organisations should always offer an opt out from the marketing.

Part 4: rights

This part is titled 'principles and obligations' but it also includes individual rights. However, there is some confusion which could be resolved by putting the individual rights into their own section.

Section 23(1) lists a set number of rights: information, access, objection, correction and deletion. However, part 4 expands on some but not all of these rights, but there does not seem to be a separate provision on the access right. In addition, some sections reference rights not in the list at section 23(1). Section 6 of the policy document has an even longer list of rights including ones that really are controller obligations rather than individual rights. It may be worth considering whether section 23(1) needs amending to include all the rights listed in part 4.

Some sections have information on timescales and some do not. It may be helpful to have one section setting out the required response timescales for all the rights.

With regards to section 34 on the right to portability, it is crucial to ensure the security and reciprocity of portability. That means that organisations on each side should have strong privacy and security measures, such as encryption in transit, to guard against unauthorised access, diversion of data or other types of fraud. It is also important that an individual's decision to move data to another provider should not result in any loss of control over that data. It should be noted that to realise such security and reciprocity, it is important to encourage private-sector initiatives to develop applicable standards that will provide for greater flexibility than prescribed formats or other relevant rules on portability being defined by public bodies.

The policy document also sets out that there can be limits on rights in some circumstances, but these are not covered in the draft Bill.

Part 4, section 37(2)(c): security

To give effect to subsection (1), the data controller or data processor shall take reasonable measures to:
(c) [implement] the pseudonymisation and encryption of personal data;

It is important to note that pseudonymisation and encryption are not always appropriate and can hinder the business activity in question. For example, it is very difficult to carry out searches of databases where there is record-level encryption. It may be helpful to add to this clause to indicate that these measures should be used where they are appropriate, rather than mandating them as a core part of all security.

Part 4, section 38: breach notification

The provisions on breach notification have no threshold for reporting breaches either to the Commissioner or the individual.This presents a real risk of the Commissioner being overwhelmed with reports and individuals worried unnecessarily if the breach turns out not to have compromised personal data, or not in the way first thought. Experience from the US also shows that without a threshold individuals experience 'breach fatigue' where they no longer pay attention to notifications they get.

It would be helpful to specify that notification is required where there are significant risks to the individual. The EU approach has been to mandate notification of breaches to the Commissioner unless there are no risks to the individual; and to mandate notification to individuals where there is significant risk.

The provision in the draft Bill also requires both controllers and processors to report breaches, but there is no obligation on a processor to report a breach to the controller they are working for. Controllers need to know where their processor has had a breach so they can take appropriate action against the processor as needed and so they can better manage the relationship with their customers, who may be surprised to receive notifications from a processor they have no awareness off, as it is simply providing a back-office business activity to the brand they have a relationship with. In general, the controller is the person making the decisions about the personal data and when to outsource it, so they should bear the notification responsibility towards the Commissioner and individuals, rather than the processor.

Part 4, section 38(5)(d): information to individuals for breach

38 (1) Where there is a breach of security of personal data or there is reasonable ground to believe personal data has been accessed or acquired by unauthorised person, the data controller or data processor, within prescribed period, shall—
(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data.

Revealing the identity of the individual who accessed or acquired the data could in itself lead to a breach of privacy or a risk of harm to the individual. If this provision is kept, it should clarify that an organisation can reveal the identity of the unauthorised person only where to do so would not breach the data protection law or any other relevant law. Or, for example, if there is a police investigation and the police have requested the identity of the perpetrator be concealed. An organisation must safeguard the privacy rights of all individuals and must take care not to take action that could lead to harm, such as attacks on the person responsible for the breach.

Part 4, section 38(6): exemption from breach notification

(6) The notification of a breach of security of personal data shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.

It is sensible to have an exemption from breach notification where the personal data have been protected in a way that would make it impossible or very difficult to access or use. However, the provision as drafted provides a wide exemption where an organisation makes the decision that their general security measures are good enough. Whereas the key point is whether the data was protected in such a way that those accessing it unlawfully can do nothing with it.

The provision also provides an exemption from all reporting, whereas it may be more appropriate to provide an exemption from reporting to individuals, as it is in the Commissioner's interests to understand what breaches are happening and why, and what good practice to promote as a result. It may be worth considering rewording this clause to something like:
(6) The notification of a breach of security of personal data to the affected individuals shall not be required where the data controller or data processor has implemented appropriate security safeguards which make the personal data unintelligible to anyone not authorised to access it, such as encryption.

Part 5, section 40(1): typing error
This clause references section 38, but it should be section 39.
40 (1) Without prejudice to section 38 [39], ...

Part 5, sections 39 and 40: sensitive data
These sections are very confusing and contradict each other. Section 39 says to process sensitive data then section 27 has to apply, which are the grounds for processing 'ordinary' (not sensitive) personal data. Usually, the main reason for creating sub-categories of personal data deemed as sensitive is that they are to be treated differently. This is not the case if the same grounds for processing are available for both general and sensitive data.

Section 40 says 'without prejudice to section 39…' and then lists additional grounds for processing sensitive data. The effect of this is that there are more grounds for processing sensitive data than for processing ordinary data, whereas it is usually the other way round.

The EU approach has always been to require that there is first an ordinary grounds for processing the data and then, where it is sensitive, an additional ground is needed from a separate list. This may have been the intention in the draft Bill and it may just be a question of tightening up the language, so it is clear that section 40 contains the grounds for processing sensitive data.

If this is the intention, it would be sensible to also include sensitive data grounds of:
- consent;
- necessary for the performance of a contract;
- employment purposes;
- necessary as a security measure as part of verifying identity.

Part 5, section 43: other categories and grounds for sensitive data
43 (1) The Data Commissioner may prescribe further categories of personal data which may be classified as sensitive personal data.
(2) Where categories of personal data have been specified as sensitive personal data under subsection (1), the Data Commissioner may specify any further grounds on which such specified categories may be processed, having regard to—

It is unusual to provide the data protection authority with the ability to specify additional categories of sensitive data or additional grounds for processing, rather than these being set out in law after the normal legislative process. Organisations also need legal certainty to carry out their business and to do so in a way that is compliant with the data protection law, and the Commissioner deciding at will on new categories of sensitive data or grounds for processing sensitive data provides only uncertainty and the cost and burden of potentially constantly having to change systems and processes. It is though sensible to have a provision in the Bill allowing for the Commissioner to recommend additional categories or grounds that can then be proposed in additional regulations.

Part 6, section 44: transfers

There is significant confusion with the different provisions on transfers contained in the Bill. Section 22(1)(h) sets out a general principle that "personal data shall not transferred outside Kenya, unless there is adequate proof of adequate data protection laws by the recipient country." However, section 44 then requires local storage of a copy of personal data, and only local storage of certain personal data, yet to be decided. It also prohibits any cross-border processing of sensitive data, It then provides some grounds where you can transfer personal data outside Kenya.

The definition of 'cross-border processing' also has an impact, and the cumulative effect of the definition and the provisions would potentially prevent an organisation from processing HR data outside Kenya. This is not a feasible position for those organisations who are multinationals or who have a presence in multiple countries including Kenya. It also has a significant impact on start-ups and SMEs who cannot scale and grow their business if they are required to build or use data centres in Kenya rather than be able to use the secure set up they already have in place.

For Kenya to maintain and attract business and participate in the digital economy it is important to get the rules on data flows and cross-border transfers right. The free flow of data is a key element of economic growth. This fact has been supported by multiple studies[1]. Indeed, over the past decade, cross-border data flows have boosted global GDP by 10.1%[2].

Data localisation requirements, including the general obligation to store a copy of data in Kenya and to process 'critical data' only in Kenya, do not serve to improve data protection, severely disrupt operations of both controllers and processors and will have a negative impact on Kenya's data economy.

In many cases, it is not possible to process all data locally and maintain the same quality of service as could otherwise be achieved (for example, round-the clock, follow-the-sun customer service).

---

1 A recent study published by GSMA summarises existing studies regarding the value of data flows. See Annex B of "Regional Privacy Frameworks and Cross-Border Data Flows — How ASEAN and APEC can Protect Data and Drive Innovation", GSMA, September 2018, available at https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

2 See "Digital Globalization: The New Era of Global Flows", James Manika et al., McKinsey Global Institute, March 2016, available at https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx

The trend towards micro-services in service architecture and increasing distribution of data processing means that data localisation restrictions are likely to result in companies choosing not to serve the Kenyan market or significantly reducing the functionality of their services.

Data localisation restrictions risk significantly impairing innovation by raising costs to potentially prohibitive levels for small and medium enterprises.

Data localisation restrictions undermine Kenya's ability to leverage emerging technologies that rely significantly on global and distributed networks, like cloud computing, data analytics and AI/ machine learning.

Data localisation requirements create complex conflict of laws situations with other data protection laws globally, especially the GDPR. For example, holding data longer than necessary or using data for different purposes than for which it was originally collected (including for localisation requirement purposes), would likely be a contravention of the GDPR.

Data localisation is a costly effort that impacts on an organisation's ability to operate with consistency and to invest in focused data security measures. The more fragmented the location of the data, the greater the corresponding risks to the data being compromised given the additional and unnecessary 'touch points'.

Data localisation obligations may further weaken security by reducing the probability of network redundancy whereas a distributed network is crucial for securing data, making it possible for data to be restored in case of data loss caused due to natural disasters or cyber-attacks.

Section 44(1) provides that a copy of all personal data be kept in Kenya. Such a localisation requirement would impose significant costs on companies of all sizes operating in Kenya, both foreign and domestic, and is not necessary to ensure privacy protections for such data. On the contrary, the requirement to maintain a serving copy in Kenya would force foreign companies to use or create data storage facilities within Kenya, thereby creating substantial additional security risks and threats of leakage and thus compromising user privacy. This requirement would also lead a move towards centralisation of data storage, which would be extremely dangerous from the point of view of harm likely to be caused by a potential cyber-attack.

Cross-border data flows should be protected, and the appropriate level of privacy protection for personal data flowing across borders ensured, through an 'adequacy' finding of a country or international organisation, or a sector within a country, or through technical and legal measures, including contracts and/or accountability-based frameworks such as enforceable corporate rules, codes of practice, codes of conduct and certifications. The addition of a mirroring requirement as contained in Section 44(1) is unlikely to serve this purpose. The objective behind the inclusion of this requirement is not clear, and may not be proportionate to the burden and risks being imposed.

One of the possible reasons for the data localisation requirement in the draft Bill may be the need to secure the lawful access to data in cross-border investigations of serious crimes. Given the consequences of data localisation requirements as described above, it is more effective for the Kenyan government to encourage bilateral and multilateral instruments to make data sharing work in such instances without resorting to localisation. For example, the CLOUD Act recently enacted

by the US enables bilateral agreements with qualifying countries which would allow non-US qualified governments to get access to data in the context of criminal investigations in a much more efficient way. Kenya should aim for these types of agreements to resolve such issues while avoiding the negative economic impact of data localisation. This issue has also been dealt with in trade agreements, such as the recent US-Mexico agreement whereby financial institutions are no longer required to store data locally as long as the relevant authorities are able to access the information they require.

Section 44(2) provides that "The Cabinet Secretary shall prescribe, based on grounds of strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data centre located in Kenya".
Other than in very narrow, thoroughly justified and specific cases related to State security, classified information or national defence related matters, such an extreme localisation measure is not necessary to protect personal data, nor is it necessary to ensure proper access to data by the authorities. Both objectives can be achieved through technical and legal measures that do not impose similar unnecessary costs on efficient economic activity within Kenya.The Kenyan Indian market could be hampered by data localisation obligations which will reduce options for Kenyan companies, especially small and medium size players who rely on Kenya's current open and free data flow policy to compete with international players who have access to cutting edge technologies and tools in accessing various markets.

For example, many businesses rely on 24-hour customer service. That requires access to personal data outside of Kenya's time zone. It would not serve Kenya well to force companies to choose between functionality and efficiency on the one hand or establishing or maintaining a business presence in Kenya on the other. Both should be possible. It would also not serve Kenyan companies well that would like to expand beyond the Kenyan market or do business with such companies. It can also stifle international research efforts and prevent advancement in key sectors of the global economy (such as international medical research).

Apart from the very narrow and specific cases mentioned above, it is not advisable for a data protection law to include such special categories of data that can only be processed in Kenya.

The transfer provisions would benefit from further discussion to understand what they intend to achieve and to determine whether mandating localised data storage is the right approach.

Part 7, section 49: research, history and statistics
49 (1) The further processing of personal data for a research purpose in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained.
(2) Personal data which is processed for research purposes in compliance with the relevant conditions may be kept indefinitely.
(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if—
(a) data is processed in compliance with the relevant conditions; and
(b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

This section seems to be similar to an equivalent provision in the UK Data Protection Act 1998. However, it references 'relevant conditions' without specifying what those are.
In the UK Act, the relevant conditions are:

(a) that the data are not processed to support measures or decisions with respect to particular individuals, and
(b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

The other main difference from the UK Act is that in section 49(3), research processing is exempt from the entire Act, whereas in UK law this aspect relates only to an exemption from the right of access. It seems unnecessarily wide to exempt research processing from any governance obligations. As a minimum organisations should have to tell individuals that their personal data will be used for research as part of transparency obligations and they should be compelled to keep the data secure. They should also have to comply with the main data protection principles set out in section 22 (except 22(1)(g) as per the previous comment on this point).

Part 8: enforcement provisions

The Commissioner only seems able to investigate complaints; there are no provisions on how they enforce breaches of the law in terms of process or penalties. For example, a system of assessments, audits, warning notices, enforcement notices and appeals.

It would also seem sensible to have all the offences together in one place, rather than scattered throughout the Bill.

Suggestions for additional provisions

- Access right

This is often considered the key right for individuals as it is only with the ability to find out what data an organisation holds about you that you can discover if there are inaccuracies or you can exercise other rights in relation to the data. Therefore, it is surprising to find there is no separate provision in the draft Bill setting out the details of this right, even though there is some mention of it in the policy document. As access rights can be used as a weapon against organisations it is also important to include provisions that where an access request is manifestly unfounded, excessive, technically impossible or vexatious, then an organisation should be able to refuse the request or charge a reasonable fee to assist with complying with the request. In cases where the controller refuses the request, it must be able to (1) demonstrate the manifestly unfounded, excessive or vexatious character of the request and (2) justify its decision.

- Accountability

Although set out as a principle in the policy document, there are no provisions in the draft Bill. Kenya has in its policy document rightly recognised, along with most other data protection regimes, that this is an important concept. Accountability puts responsibilities on organisations to handle personal data properly and lawfully and to be able to demonstrate their efforts on demand. It places an ex-ante burden to protect individuals on the organisation (by implementing measures that correspond to all elements of accountability and/or the corresponding legal requirements), subject to ex-post enforcement by the data protection authority.

There are two excellent papers worth looking at on this topic from CIPL (Centre for Information Policy Leadership). The first of the two papers explains, among other things, the essential

elements of accountability and how they can be implemented and demonstrated by organisations. The second paper addresses how data protection authorities and policy and law makers can specifically incentivise organisational accountability beyond the incentive that comes from having to comply with legal requirements.

The essential elements of organisational accountability - leadership and oversight, risk assessment and DPIAs, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement - directly correspond to the requirements of most data protection laws. For the sake of global harmonisation, consistency and interoperability, it is important that there be broad consensus and a common understanding of the concept of accountability and how it should be deployed. A proper application of the concept of accountability would improve the effectiveness and efficiency of Kenya's data protection regime by reducing the ex-ante tasks and administrative burdens of the data protection authority (such as authorising, approving, specifying or notifying various items) and leaving these issues to the accountability obligations of the controllers, subject to ex-post enforcement. In addition, when implemented correctly, organisational accountability enables an effective data protection framework that reduces the burden on individuals to protect themselves in the complex digital economy.

"The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

"Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf