Submissions on the Privacy & Data Protection Policy 2018

This submission reflects specific comments and recommendations on the "draft Policy".

European Union-General Data Protection Regulation (EU-GDPR)

Comment: Whilst the "draft Policy" is heavily borrowed from the EU-GDPR, we do not think there is a one-size-fits-all approach to privacy. IBM has long recognized the power data holds for our clients. It is the key to their competitive advantage. Today, it's powering AI systems, helping companies develop deeper insights, unlocking new discoveries and making decisions exponentially faster. However, as more and more organizations interact with and manage data, all have an obligation to do so RESPONSIBLY as we have outlined previously in our high-level recommendation for both the "draft Policy" and "draft Bill".

What works for one country or region will not necessarily work for another. IBM has worked closely with the EU to ensure the GDPR addresses privacy concerns without undermining innovation, and we appreciate the EU's desire to provide a unified approach across the EU and bring outdated regulations in line with 21st century challenges. But we do not agree with every component of the GDPR. As other countries consider their own privacy challenges, we do not believe that GDPR should be simply grafted onto privacy systems where its relatively prescriptive approach may not work.

Instead, IBM believes nations should pursue a third way–one with a track record of success. Instead of government mandates, we believe a collaborative public-private approach, led by industry together with government, is the most feasible way to develop a framework of data privacy standards tailored to the nations' needs. Data privacy is a global priority, but one that must be addressed locally. We applaud Europe for taking early action. Yet a different – but no less effective – approach may be the best way to assure Kenyans that their digital privacy is being protected.

Section 2: Purpose of the Policy

IBM works with governments around the world to encourage policies that foster innovation, protect intellectual property, and encourage use of technology to address important societal needs. With Kenya being one of the many countries in the African region seeking to become a data/ICT hub – home of the African "Silicon Savannah" - and ranked one of the most innovative countries in Africa, it would be useful for the policy statement to recognize this objective, as privacy interests do not exist in a vacuum, and must always be balanced with other constitutional rights such as the freedom of expression, access to information, consumer rights and other societal interests, such as innovation and economic prosperity, and the corollary need for organizations to process personal data for legitimate business purposes.

Recommendation: Canada's and Singapore's privacy laws for example state that *"The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."*

3. Section 4. Scope

Our concern is drawn to this wide scope of the policy, which could lead to conflict with other countries' data privacy laws and may negatively impact Kenya's ability to attract foreign business and grow its ICT industry. Clause 4.4. in our view would basically cause Kenyan law to apply to personal data owned by a foreign company about individuals with no nexus to Kenya to the extent that this data is processed in Kenya by a data processor. For example, a German hotel chain (data controller) not established in Kenya doing business with a Kenyan service provider (data processor) would now automatically be subject to Kenyan privacy law, simply by virtue of having its data processor established in Kenya; this of course on top of the GDPR, which is the law that would apply to the German company because of its EU establishment. This could result in conflict of law for the German company, not to mention an increased regulatory burden.

Recommendation: Kenyan data privacy law should rightly apply to personal data of individuals located in Kenya and processed by a data controller located in Kenya. As is the case with the GDPR, it should also apply to data controllers located outside of Kenya to the extent that there is a demonstrable targeting of individuals located in Kenya (e.g. an American university promoting itself on a Kenyan website and collecting personal data of students in the process). However, it should not over-reach to apply to instances where personal data about individuals not located in Kenya are involved. Such situations should be dealt with by laws which are applicable in the country where the individual is located. It's a matter of 1) trying to avoid conflict of laws, 2) encouraging the growth of ICT sector in the country and 3) focusing data privacy law enforcement resources supported by Kenyan taxpayers on matters involving individuals located in Kenya, as opposed to individuals located in other countries.

Section 5. Principles for Data Protection

1. Fairness, Lawfulness and Transparency:

(i) Clause 5.1.3 states: "Personal data will be considered to have been obtained fairly if the data subject is informed of the name of the data controller and the purpose(s) for processing the personal data or any further……"

Comment: When IBM collects personal data about prospects or clients, it makes this data available to our IBM Business Partners to allow them to pursue an opportunity. From experience, it is not practical to identify in each single case the Business Partner by name to the individual whose data we are passing onto them. But we certainly do let our prospects and clients know that as part of pursuing an opportunity, we may make their personal data available to our Business Partners. Hence, replacing the word "name" with "identity" in this clause, provides a bit more leeway for data controllers.

Recommendation: Amend as follows… Clause 5.1.3: "Personal data will be considered to have been obtained fairly if the data subject is informed of the identity of the data controller and the purpose(s) for processing the personal data or any further……"

(ii) Clause 5.1.4 states: "Data controller/processor should be transparent regarding the processing of personal data and inform the data subject in an open and transparent manner. Personal data should only be processed if and only if there is a legitimate

purpose for the processing of that personal data. A Data controller/processor should practice transparency so that the data subjects will be sufficiently informed regarding the processing of their personal data. When processing personal data, the individual rights of data subject must be protected."

Recommendation: Expunge references to "data processor" in the clause. Data processors' role is to process data that is controlled by the data controller, as per the data controller's instructions. Data processors do not have, in any privacy law, an obligation to provide notice/be transparent nor are they responsible for determining whether there is a legitimate purpose for processing the data. This is the responsibility of the data controller. Often, data processors will not even know whose data they are processing, let alone the circumstances of the processing.

2. Purpose Limitation:

(i) Clause 5.2.2 under the 'Purpose Limitation' principle reads: "Personal data must be processed only for the purpose that was defined before the data was collected."

Recommendation: Amend to read: "Personal data must be processed only for the purpose that was defined before the data was collected and for compatible purposes."

(ii) Clause 5.2.3 under the 'Purpose Limitation' principle reads: "Further processing for archiving purposes in the public interest, scientific interest or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose. Subsequent changes to the purpose are only possible to a limited extent and require legitimate basis."

Comment: We are unclear as to what an "archiving purpose" is. Can the same conclusion be achieved than the one originally sought by removing the term?

3. Accuracy:

(i) Clause 5.5.1 reads: "Personal data on file must be correct, complete, and be kept up to date."

Recommendation: This requires qualification with an amendment to read: "Personal data on file must be correct, complete, and be kept up to date commensurate with the purpose for which it is used." Not all data requires the same level of care in this regard. Contact data used for marketing purposes certainly does not require companies to take any steps to ensure its ongoing accuracy. Data used however to determine someone's credit score should definitively be as accurate as possible.

(ii) Clause 5.5.2 reads: "Suitable steps must be taken by a data controller to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated."

Recommendation: Similar to the previous comment, this requires qualification with an amendment to read: "Suitable steps must be taken by a data controller to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated commensurate with the purpose for which it is used." Also, there will be clear exceptions to this requirement that will need to be added, such as when the there is a dispute, or a law requires the data to be kept.

4. Accountability:

(i) Clause 5.7.1 reads: "All Data Controllers/Processors shall be responsible for personal data protection and be able to demonstrate compliance to the principles on Data Protection."

Recommendation: Similar to our earlier recommendation at Clause 5.1.4, expunge reference to data processors. Data processors only act on behalf of the data controllers. They do not own the personal data and are not responsible for determining the means of processing. If they were, they would become data controllers of their own rights, which is not a desirable result. Can you imagine an IT service provider (data processor) performing a service on behalf of the Kenyan Government, and taking on the responsibilities to provide notice to Kenyans pertaining to how their data is processed by them, determining whether the Kenyan government has a legal basis for collecting personal data from Kenyans, determining whether and how Kenyans should have access to their data, etc.?

Section 6. Data Subjects Rights

Comment: As earlier stated, this "draft Policy" particularly appears to be an attempt to summarize the provisions of the EU's GDPR. However, as it lacks any amendments and recitals like what is in the GDPR that would put these provisions into context, it risks being nearly impossible to implement. Consequently, all of these data subject rights, copied from the GDPR, will need to be subject to exceptions or further qualified, as they are in the GDPR. For example, requiring the regulator to be notified about all data breaches without any threshold will likely overwhelm the regulator.

Section 7. Legal Grounds for Processing

(i) Clause 7.2.1. reads: "Data Controller/Data Processor will obtain consent from Data Subject on the processing of Personal Data including sensitive personal data."

Recommendation: Expunge reference to "data processor". Data processors do not obtain consent. It is the data controller's responsibility to determine the appropriate legal basis for processing, and to implement it. Processors are at the service of the Controllers... They have no rights to the data, including the rights to determine how the data will be processed.

(ii) Clause 7.2.3 reads: "The processing of personal data for a child shall be done only with the consent of the child's parent or guardian."

Recommendation: Define what a child is. What age triggers this requirement?

(iii) Clause 7.3.1 reads: "The policy acknowledges that there will be exceptional circumstances where personal data can be processed without the data subjects' consent. There may be limitations on data subject rights when required by the law or when there are competing rights and therefore it will require an assessment based on the facts and circumstances."

Comment: There are a number of issues with this exceptions approach. This "draft Policy" from our understanding is also meant to apply to public sector entities. The reality is that most of the processing performed by these entities could not occur if they were subject to citizens' consent. All public sector privacy laws out there contemplate that governments have the right to process data as long as it is in support of their public mandate. Consent should be one of the legal basis available to organizations to process personal data. Under the GDPR for example, organizations can process data if:

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
3. processing is necessary for compliance with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

(iv) Clause 7.4.1 reads: "Personal data shall not be disclosed or processed by a third party except when required by law or the third-party Data Processing Agreement has been approved and signed by the Data Controller and the Data Processor (i.e. the third party) and the Data subject is aware of this arrangement."

Comment: Why would the data subject need to be made aware that there is a contract between the organization (e.g. bank) they have a relationship with and the bank's service providers? Rather, there should be a requirement for such an agreement to be in place, without any need to notify data subjects of such, as such would be expected and indeed required.

(v) Clause 7.5.1 reads: "This policy may allow personal data to be transferred to other countries or entities if such countries or entities have met the adequate safeguards spelt out in this policy for maintaining the required protection for the privacy rights of the data subjects in relation to their personal data."

Recommendation: We encourage the Government not to enact restrictions on cross border data flows but instead, require covered organizations to remain accountable when transferring personal data to other countries for processing, and to adopt measures to ensure that the transferred personal data is processed as per Kenyan law.

If this fails, then we should encourage the Government t to make a robust list of data transfer mechanisms available. Please refer to: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf

Section 8. Obligations for Data Processing

(i) Clause 8.2.6. reads: "Notify the regulator of any data breach."

Recommendation: Only breaches where there is a real risk of significant harm to individuals should be notified. Without this qualifier, the regulator will not be able to handle and differentiate between inconsequential breaches and breaches which should get their attention. Similarly, the administrative burden on organizations to notify every single breach (e.g. misdirected mail or email to one single individual not containing sensitive personal information) would add cost without any associated benefits for individuals.

(ii) Clause 8.2.7. reads: "Register with the data protection regulator."

Section 11. Monitoring and Evaluation

(i) Clause 11.4. reads: "Data Protection Officer will make regular compliance reports to the Office of the Data Protection Regulator on data protection."

Comment: IBM find this provision a novelty as we have never seen any privacy law imposing an obligation on a company to make regular compliance reports. How is this going to be enforced? What is the regulator going to do with this information? Will they have the staffing and expertise to make sense of it? Compare trends? Take actions? This provision seems highly impractical and is actually not necessary since, due to the principle of accountability, the data controller has to document and prove compliance in case of need.

Appendix A: Definition of Terms

Recommendation: Amend these definitions as follows:

Data controller: A person who either alone or jointly with other persons or in common with other persons or as a legal duty determines the purpose for and the manner in which personal data is processed or is to be processed.

Data Processor: In relation to personal data, any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller.

Submissions on the Data Protection Bill, 2018

This submission reflects specific comments and recommendations on the "draft Bill".

The Data Protection Bill, Senate Bill No. 18 of 2018:

Comment: IBM formally issued on July 30, 2018 its submissions to the Senate's Standing Committee on Information and Technology on the "The Data Protection Bill, Senate Bill No. 18 of 2018". Consequently, it is our hope that as-is the typically the procedure when two competing Bills are published, that your Ministry and the Senate will work together to harmonize the two draft Bills and their collective submissions from the various public participation processes as provided by the Constitution. To this end, we have attached our submissions to the Senate's Bill to avoid the need for repetition of any concerns raised in this Bill that relates to the "draft Bill", the subject of review and comment of this submission.

That said, and to effectively protect privacy and to meet international standards in protecting personal data, we appreciate that our review of the "draft Bill" has strived to remedy/cure several issues, concerns, ambiguities and omissions within the Senate Bill as outlined below under each Part of the Bill as set out below:

- ✓ Clarifying and expanding the definitions under Clause 2 - Interpretations outlined in Part I, for example:
  - ➢ Introducing the definitions of anonymization, biometrics, consent, cross-border processing, data processor, health data, profiling, pseudonymization, Third-party
  - ➢ Expanding the definition of data controller to include both private and public entities
  - ➢ Clarifying the definition of data subject as a natural person; and
  - ➢ Expanding the definitions of sensitive personal data to include genetic data, sex life or sexual orientation
- ✓ Providing for in Part II - Office of The Data Protection Commissioner – to be established as a body corporate that is administratively and financially independent of any public authority and is given the necessary powers and adequate resources to conduct its mandate as an oversight and enforcing mechanism for this law.
- ✓ Providing in Part III the process of registration of data controllers and processors
- ✓ Reviewing the material and territorial scope of the law with the aim of clarifying that the law applies to public entities including law enforcement and intelligence agencies.
- ✓ Providing in Part IV all data protection principles including fairness and transparency, data minimization and accountability; guaranteeing that data subjects are provided with rights including the right to suppress or block (restrict), the right to data portability, as well as the protection and enjoyment of their rights in relations to profiling and automated decision making; clarifying the obligations imposed on data controllers under Clause 26 - Duty to Notify.

Part I – Preliminary

(i) Clause 2 on "Interpretation" states: In this Act – "anonymization" means the irreversible removal of personal identifiers from personal data so that the data subject is no longer identifiable;

Comment: This is not a reasonable standard for anonymization. With advances in technology, it is almost impossible to guarantee that data will never be re-identified. The Federal Trade Commission (FTC) came up with a much more practical test in its 2012 report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers". The report explains that "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." With respect to the first prong of the test, the FTC clarified that this "means that a company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device." Thus, the FTC recognizes that while it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is a reasonable basis to believe that the remaining information in a particular record cannot be used to identify an individual.

(ii) Clause 4 (1) (b) on "Application" reads: "This Act applies to the processing of personal data — to a data controller or data processor who –

(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or

(ii) not established or ordinarily resident in Kenya, but uses equipment in Kenya for processing personal data, other than for the purpose of transit through the country"

Recommendation: Kindly refer to our previous comments and recommendations on Scope under the "draft Policy".

Part II – Office of Data Protection Commissioner

(i) Clause 5 (1) (3) reads: "The Office shall comprise the Data Protection Commissioner as its statutory head and accounting officer, and other staff appointed by the Data Commissioner."

Recommendation: Drafters have used the terms "Data Commissioner" and "Data Protection Commissioner" interchangeably in several subsequent clauses [see (ii) and (iii) below], which should be corrected.

(ii) Clause 7 (1) (b) reads: "The functions of the Data Commissioner shall be to - establish and maintain a Register of data controllers and data processors"

Comment: IBM's experiences in other jurisdictions have shown that there is little merit to the approach of having organizations register with a Data Protection Authority (DPA). First, most organizations ignore the requirement, especially small- and medium-sized businesses. Secondly, the DPA does not have the manpower to police the registry.

(iii) Clause 7 (1) (g) reads: "The functions of the Data Commissioner shall be to - carry out inspections of public and private entities with a view to evaluating the processing of personal data"

Comment: Such inspections should be subject to some kind of a trigger (such as the fact that the DPA has reasonable grounds to suspect that the law may be breached).

Part IV – Principles and Obligations of Personal Data Protection

(i) Clause 22. (1) reads: "Every data controller or data processor shall ensure that personal data is–…."

Comment: These are responsibilities of the Controller. Processors cannot fulfill these responsibilities, as they are entities merely acting on behalf of the Data Controller they provide a specific service to, as per their instructions. A data processor that merely stores personal data on behalf of a controller for example would never be in a position to acquit these duties vis-a-vis the controller's personal data.

Recommendation: Expunge reference to "data processor" in this clause.

(ii) Clause 22 (1) (d) reads: "Every data controller or data processor shall ensure that personal data is– adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed"

Recommendation: Propose that the clause be amended to read: ""Every data controller shall ensure that personal data is– adequate, relevant, limited to what is necessary in light of the purpose for which it is to be used, accurate and kept up-to-date and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay."

(iii) Clause 22 (1) (g) reads: "Every data controller or data processor shall ensure that personal data is - only released to a third party only with the consent of the data subject; and"

Recommendation: This does not make sense, considering the definition/interpretation of "third party" earlier in Part I-Preliminary in the "draft Bill". For example, an organization would then need consent to release personal data to a public authority pursuant to their legal mandate (law enforcement agency, revenue agency, etc.). Therefore, an amendment to this clause is required to allow for the principle of lawful processing under any of the legal bases identified in the GDPR.

(iv) Clause 22 (1) (h) reads: "Every data controller or data processor shall ensure that personal data is - not transferred outside Kenya, unless there is adequate proof of adequate data protection laws by the recipient country.

Recommendation: We consider the provisions of the above clause as too restrictive. The presence of adequate laws in a country should not be the only data transfer mechanisms available. Therefore, this clause requires an amendment to provide for a more diversified toolkit of mechanisms to transfer data to third countries beyond adequacy decisions including: standard contractual rules, binding corporate rules, certification mechanism, codes of conduct, model clauses, so-called "derogations" or other appropriate safeguards of protecting personal data when made available outside the country of origin.

(v) Clause 23 (1) reads: "A data subject has a right to-"

Comment: The rights under this section are not absolute. Provision needs to be made for their corresponding exceptions, as is the case with the GDPR.

(vi) Clause 23 (1) (b) reads: "A data subject has a right to - access their personal data in custody of data controller or data processor;"

(vii) Clause 25 (1) reads: "A data controller or data processor shall collect personal data directly from the data subject."

(viii) Clause 25 (3) reads: "A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.

(ix) Clause 26 (1) reads: "A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject –"

(x) Clause 27 (1) reads: "A data controller or data processor shall not process personal data, unless –"

(xi) Clause 27 (3) reads: "Where processing operation is likely to result in a high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out an impact assessment of the envisaged processing operations on the protection of personal data.

(xii) Clause 28 (1) reads: "A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of his personal data for a specified purpose."

(xiii) Clause 29 (1) reads: "Every data controller or data processor shall process personal data of children in a manner that protects and advances the rights and best interests of the child."

(xiv) Clause 29 (2) reads: "A data controller or data processor shall incorporate appropriate mechanisms for age verification and parental consent in order to process personal data of children, such mechanisms determined on the basis of -"

(xv) Clause 30 (1) reads: "A data controller or data processor may, at the request of a data subject, restrict the processing of personal data where –"

(xvi) Clause 32 (1) reads: A data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate grounds for the processing which overrides the data subject's interests, rights and freedoms or for the establishment, exercise or defense of a legal claim.

(xvii) Clause 33 (1) reads: "A data controller or data processor shall not provide, use, obtain, procure personal data of data subject for the purpose of direct marketing without prior consent of the data subject."

(xviii) Clause 34 (1) reads: "A data subject has the right to receive personal data concerning them, which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format."

(xix) Clause 35 (1) reads: "A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is -"

(xx) Clause 36 (1) reads: "A data subject may, subject to exemptions under this Act, request a data controller or data processor to –"

(xxi) Clause 36 (1)(b) reads: "erase or destroy personal data that the data controller or data processor is no longer authorized to retain, irrelevant, excessive or obtained unlawfully."

(xxii) Clause 36 (2) reads: "Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the -"

Comment: The obligation on the processor should be to notify the controller if they receive an access request from the individual. Additionally, the requirement to provide access should lie with the data controller, who "owns" the data. We therefore, hold the view that the requirements/obligations stipulated in the respective clauses in (vii)-(xxii) are not for the data processor. The data processor should only collect as per the instructions of the data controller on whose behalf they do the collection (as applicable).

Recommendation: Expunge the words "data processor" from the respective clauses in (vii)-(xxii) above.

(xxiii) Clause 26 (1) reads - "A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject –

(b) the fact that personal data is being collected;
(g) consequences if any, where the data subject fails to provide all or any part of the requested data."

Recommendation: Amend the above two sub-clauses to include the words "unless obvious" and read: Clause 26 (1) states - "A data controller shall, before collecting personal data, in so far as practicable, inform the data subject –

(b) the fact that personal data is being collected unless obvious;

(g) consequences if any, where the data subject fails to provide all or any part of the requested data unless obvious."

(xxiv) Clause 27 (4) reads: "A data controller who contravenes the provisions of section (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five million to imprisonment for a term not exceeding five years.

Comment: In our opinion, imprisonment should be reserved for cases where there is a criminal element involved (e.g. individual behind a cyber-attack that causes harm to individuals; theft of data) and not for a mere non-compliance event (e.g. did not obtain proper consent or provide appropriate notice). Additionally, it is not clear what currency is contemplated when "five million" is invoked, but there has to be a better scale for breaches. Even the GDPR is more nuanced.

(xxv) Clause 28 (2) reads: "Unless as provided under this Act, a data subject shall have the right to withdraw consent at any time."

Comment: There are exceptions and nuances to this provision as drafted that must be considered. For example, even the GDPR makes the exception that where there is another legal basis for processing, processing can continue.

(xxvi) Clause 29 (2) (d) reads: "A data controller or data processor shall incorporate appropriate mechanisms for age verification and parental consent in order to process personal data of children, such mechanisms determined on the basis of—such other factors as may be specified by the Authority."

Comment: Which Authority is referred to in this clause? The Data Protection Commissioner?

(xxvii) Clause 29 (3) reads: "The Data Commissioner may appoint as guardian of the child a data controller or processor who -"

Comment: This provision does not make sense. Its logic is hard to understand.

(xxviii) Clause 30 (2) reads: "Where processing of personal data is restricted under this section –

(a) the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defense of a legal claim, the protection of the rights of another person or for reasons of public interest; and"

Comment: We note that if another legal basis can be invoked, restrictions can be overridden.

(xxix) Clause 33 (1) reads: "A data controller or data processor shall not provide, use, obtain, procure personal data of data subject for the purpose of direct marketing without prior consent of the data subject.

Comment: This is more restrictive than the GDPR. The GDPR allows for legitimate interest to be used for marketing, with the caveat that the data subject can withdraw their consent at any time.

(xxx) Clause 38 (1) reads: "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 unauthorized person, the data controller or data processor, within prescribed period, shall -"

(xxxi) Clause 38 (2) reads: "Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller within the prescribed period."

Comment: The two provisions create too low a threshold for notification of a personal data breach. The GDPR says: *"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."*

Part V— Grounds for Processing of Sensitive Personal Data

(xxxii) Clause 41 (1) reads: "Personal data relating to the health of a Data Subject may only be processed –

(a) by or under the responsibility of a professional; or
(b) by a person subject to the obligation of professional secrecy under any enactment."

Comment: We observe the following issues with this clause and its provisions as drafted. What happens when a data controller/processor collects data about employees who require special accommodations e.g. the physically handicapped or employees who need a health-related leave of absence? While we understand that the data controller/processor would not have access to the health reasons that required such special accommodations, our health benefit providers certainly would. Finally, does this clause cover the processing of personal health data in clinical trials and other scientific research situations?

(xxxiii) Clause 41 (2) reads: "The health data of a Data Subject under subsection (1) can only be processed when is necessary for -

(a) the purpose of preventive or occupational medicine;
(b) assessment of the working capacity of an employee,
(c) medical diagnosis;
(d) provision of health or social care; or
(e) treatment or the management of health or pursuant to a contract with a health professional."

Recommendation: In addition to previous comments related to this section, what about including research and clinical trials as necessary activities/situations by amending the clause to read: Clause 41 (2): "The health data of a Data Subject under subsection (1) can only be processed when is necessary for –

(a) the purpose of preventive or occupational medicine;
(b) assessment of the working capacity of an employee,
(c) medical diagnosis;
(d) provision of health or social care;
(e) treatment or the management of health or pursuant to a contract with a health professional; or
(f) scientific research and clinical trials"

(xxxiv) Clause 42 reads: "Any person who contravenes any provision in this part shall commit an offence and be liable, on conviction, to a fine not exceeding five million shillings, or to imprisonment for a period not exceeding five years."

Comment: Similar to previous comments made for Clause 27 (4) at (xxiv) above.

Part VI —Transfer of Personal Data Outside Kenya

(xxxv) Clause 44 (1) reads: "Every data controller or data processor shall ensure the storage, on a server or data center located in Kenya, of at least one serving copy of personal data to which this Act applies."

(xxxvi) Clause 44 (2) reads: "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 center located in Kenya."

(xxxvii) Clause 44 (3) reads: "Cross-border processing of sensitive personal data is prohibited."

Comment: We question the logic of the data localization requirements expressed under Clause 44 (xxxv-xxxvii above). Is the purpose to provide easy access to local surveillance/enforcement agencies? In our view, this provision will create additional compliance and enforcement costs for data controllers/processors and their supervisory authorities, respectively. For this reason, any service for 'non-digital' companies will become costly compared to digital services provided outside of Kenya. This leads to a competitive disadvantage for innovative, digital businesses in Kenya, and an overall economic disadvantage for the whole economy, as any business processing data, has to make sure that they are not only stored 'in the cloud' (e.g. if using simple SaaS-services as calendar tools), but also physically on servers in Kenya.

(xxxviii) Clause 45 (1) reads: "A data controller or data processor may transfer personal data to another country where -"

Comment: Similar to previous comments made for (iv) Clause 22 (1) (h) at above.