SUMMARY COMPARATIVE ANALYSIS OF THE KENYA DATA PROTECTION BILLS, 2018.

BY

LUCY NJOKI MWANGI

njokiluc@gmail.com

LLB (HONS) KABARAK UNIVERSITY
PGD KENYA SCHOOL OF LAW
LLM Candidate, (LAW, SCIENCE & TECHNOLOGY) UON*

This document is a summary of a comparative analysis of the Senate and MoICT Task Force Draft Data Protection Bills and is not intended to be relied on as legal advice.

1. Table of Contents

1. Introduction

The Constitution of Kenya in Article 31 provides for the right to Privacy in the following terms:

> ***31***. *Every person has the right to privacy, which includes the right not to have-*
>
> *(a) their person, home or property searched;*
> *(b) their possessions seized;*
> *(c) information relating to their family or private affairs unnecessarily required or revealed; or*
> *(d) the privacy of their communications infringed.*

In order to give effect to Article 31 (c) and (d), the Senate Committee on Information Communication and Technology developed and published a Bill, the Data Protection Bill 2018 (hereafter referred to as the Senate Bill) and invited public comments. The Cabinet Secretary of the Ministry of Information, Communications and Technology also set up a Task force which came up with a Bill, the Data Protection Bill 2018 (hereafter referred to as the Task Force Bill) to give effect to Article 31 (c) and (d). This is a summary comparison of the contents of the two Bills.

2. Application

The Task force bill provides for the processing of personal data (s. 4(1))-

(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means: provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;
(b) 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 the Kenya for processing personal data, other than for the purpose of transit through the country;

The Task Force Bill does not apply to (s. 4(2)) –

(a) the exchange of information between government departments and public sector agencies where such exchange is required on a need-to-know basis;
(b) the processing of personal data by an individual in the course of a purely personal or household activity; or
(c) Processing of personal data exempted under section Part VII.

The Senate bill (s. 3) on the other hand, does not apply to the processing of personal data by or on behalf of a public body-

(a) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorism and related activities, defence or public safety; or

(b) the purpose of which is the prevention, detection and identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, prosecution of offenders or the execution of sentences or security measures.

- **The Bills do not provide for any standard to be upheld for data processed outside Kenya beyond requiring an existence of data protection laws.**
- **Section 4 (b) of the Task force Bill needs to be reconsidered.**
- **There are hardly any standards that security and law enforcement agencies are held to, in both Bills, with regard to processing of personal and sensitive/special personal data.**
- **The effect of the exemptions given to public bodies (including those in s. 4(2) (a) of the Task force bill) in both Bills almost limit the scope of the Bills to personal data processed by private bodies.**

3. Principles of Data Protection

The Task force Bill and the Senate Bill both provide for the principles of collection limitation, purpose specification, use limitation and data quality in similar terms.

While both Bills provide for data retention in s. 22(f) (Task force Bill) and s. 4(e) (Senate Bill), the Taskforce Bill specifically encompasses personal data 'kept in a form which identifies the data subjects' compared to the Senate Bill's broad cover of 'information' as that which should not be kept for longer than is necessary for achieving the purpose for collection.

Whereas the Senate Bill provides for security safeguards as both a principle of data protection (s. 4h) and an obligation upon agencies (s.15), the Task force Bill only frames it as an obligation upon data controllers and processors in s.37.

Both Bills provide for the principle of data quality but the Senate bill extends the principle to include 'complete' data. Both Bills then make it an obligation on agencies to rectify incomplete data in s. 36(1) (a) of the Taskforce Bill and s.8 of the Senate Bill.

4. Rights of a Data Subject

Both Bills provide for the rights of the data subject to:

(a) be informed of the use to which their personal data is to be put;
(b) access their personal data in custody of data controller or data processor;
(c) object to the collection or processing of all or part of their personal data;
(d) correction of false or misleading data; and

(e) deletion of false or misleading data about them.

Differences

The rights of a data subject are couched in very similar terms save for the inclusion by the Senate Bill of deletion of data which has been objected to in s. 9e in addition to the provisions for the deletion of misleading and false data included in both Bills. The Senate Bill also includes the right to *an explanation in respect of the processing of data and the outcome of such processing* in s. 9f, not included in the Task force Bill.

The right of access to personal data in the custody of a data controller, processor or agency could be expanded to include the right to human intervention on the part of the controller, to express a point of view or to contest a decision. Thereafter, the data subject should have the right to obtain an explanation of a decision reached after the assessment and to further challenge the decision.

5. Collection of Personal Data

Both Bills provide for collection of personal data directly from the data subject for a purpose which is specific, explicitly defined and lawful.

In both Bills, collection is not required directly from a data subject where–

(a) the data is a matter of public record;
(b) the data subject or a competent person, where the data subject is a child, has consented to the collection from another source;
(c) the data subject has consented to the collection from another source;
(d) collection from another source would not prejudice the interests of the data subject;
(e) collection of data from another source is necessary-
  (i) for the prevention, detection, investigation, prosecution and punishment of crime;
  (ii) for the protection of the interests of the data subject or another person;
  (iii) to comply with an obligation imposed by law; or
  (iv) in the interest of national security; or
(f) compliance is not reasonably practical.

Differences

The Task force Bill (s. 25(2) (b)) provides that personal data may be collected indirectly where the data subject has deliberately made the data public and s. 25(2) (f) (ii) also in the Task force Bill further provides that personal data may be collected indirectly where collection of data from another source is necessary for the enforcement of a law which imposes a pecuniary penalty.

The Senate Bill allows agencies to collect, store or use personal data using means that in the circumstances, do not intrude to an unreasonable extent, upon the personal affairs of the data subject except as it provides or as in any other written law (s.7(3)).

The provisions that collection is not required directly from the data subject where compliance is not reasonably practical or where necessary for the enforcement of a law which imposes a pecuniary penalty are open to abuse.

The phrase 'Law imposing a pecuniary penalty' should be further defined and specific crimes listed, as both felonies and misdemeanors such as traffic offences impose a pecuniary fine.

6. Duty to Notify

In both B ills, the data subject is expected to be notified of:

(a) the fact that personal data is being collected;
(b) the purpose for which the personal data is being collected;
(c) the intended recipient of the data;
(d) contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;
(e) whether the data is being collected pursuant to any law and whether such collection is voluntary or mandatory; and
(f) consequences if any, where the data subject fails to provide all or any part of the requested data.

Differences

There is no 10(f) (f) above in the Senate Bill, (likely a typing error)

The Task force Bill further requires the data controller or processor to inform the data subject of their rights before collecting personal data in s. 26(1)(a).

The Senate Bill further requires the agency collecting personal data to specify the use to which the information collected shall be put in s. 10(1)(b) and in s. 10(1)(h) to notify the data subject of the right of access to, and correction of, personal data provided under section 13 and 15.

The rights of the data subject, as would be drawn from the principles of data protection should be made known to the data subject at the time of collection of data.

7. Security Safeguards of Personal Data

The Senate Bill includes the protection and security of personal data as both a principle of data protection (s. 4h) and an obligation upon the agency (s.15).

The Task force Bill includes protection and security of personal data protection only as an obligation upon the data controller and data processor (s.37).

Their similarities are in that the data controllers, data processors and agencies have to ensure the integrity of personal data in its possession or control through the adoption of appropriate, reasonable, technical and organizational measures to prevent—

(a) loss, damage or unauthorised destruction; and
(b) unlawful access to or an unauthorised processing.

They must also take reasonable measures to–

(a) identify reasonably foreseeable internal and external risks;
(b) establish and maintain appropriate safeguards against the identified risks;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated.

Differences

- Unique to the Task force Bill is the provision that the data controller or data processor is to take reasonable measures to the pseudonymisation and encryption of personal data (s.37(2)(c), and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (s.37(2)(c).
- The Task force Bill particularly provides for processing involving the transmission of data over an information and communication network, where a controller shall have regard to the state of technological development available (s.37(3)(a), cost of implementing any of the security measures(s.37(3)(b), special risks that exist in the processing of the data(s.37(3)(c), and the nature of the data being processed (s.37(3)(d)).

- Furthermore, where a data controller is using the services of a data processor the Task Force Bill requires the data controller to opt for a data processor who provides sufficient guarantees in respect of security and organisational measures for the purpose of complying (s.37(4)(a) and both the data controller and the data processor to enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller(s.37(4)(b).

- Lastly, uniquely provided for in the Task Force Bill, where a data processor processes personal data other than as instructed by the data controller, the data processor shall be deemed to be a data controller in respect of that processing (s.37 (5) and a

data controller or data processor shall take all reasonable steps to ensure that any person employed by him or acting under his authority, and complies with the relevant security measures.

- **The Task Force Bill prudently provides for wider security safeguards which should be retained**.

8. Notification of Security Compromises

Both bills provide for notification to the data commissioner (s. 38 Task force Bill) or Commission (s. 16 Senate Bill) as well as the data subject where there are security compromises.

The Task Force Bill provides for notification to be done within a prescribed period (s. 38 (2) while the Senate Bill requires notification be done as soon as is reasonably practicable (s. 16(a).

Under the Task Force Bill, the data controller may delay notification for purposes of prevention, detection or investigation of offences by the concerned public body (s. 38(3).

The Task Force Bill particularly lays down conditions for notification of breach to a data subject to be in writing (s.38(4)) and to provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including(s. 38(5):

(a) description of the nature of the data breach;
(b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;
(c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;
(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data.

The Senate bill requires that notification be made, but does not prescribe the mode or content of notification (s. 16 (a)) but it requires and agency to take steps to ensure the restoration of the integrity of the information system (s. 16(b).

- **The Task Force Bill allows public bodies to delay notification for purposes of prevention, detection or investigation of offences (s. 38(3). This provision may be subjected to abuse due to the vast entities that make up public bodies. It could be narrowed down to law enforcement agencies and similar agencies where early disclosure could harm an investigation of the**

circumstances of a personal data breach.

- **The notification given to the data subject should also include likely consequences of the personal data breach.**
- **There should be specific time frames for notification in order to avoid undue delay and to mitigate the consequences that could follow a security breach.**
- **Where it is not possible to provide all the information at the same time, the information should be provided in stages without undue delay and in consideration of severity of breach and nature of information**.

9. Rectification/ Erasure and Correction

Both Bills provide for rectification/ correction/ deletion of false, misleading or inaccurate data in s. 36 of the Task force Bill and s. 18 of the Senate Bill.

The Task Force Bill, however, goes further to require a data controller who has shared personal data with a third party for processing purposes to take all reasonable steps to inform the third party of the data subject's request for rectification, erasure or destruction of the personal data (s 36(2)).

The Task Force Bill also makes room for rectification of outdated and incomplete data (s.36(1)(a)) and erasure or the destroying of data the data controller or processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully (s.36(1)(b)).

The Senate Bill, on the other hand, requires a data subject to make a request to delete or destroy false or misleading data in writing, specifying the information to be collected or deleted or in the case of a request for correction to specify the manner in which such information is to be corrected.

The agency then has 7 days to consider the request and inform the data subject of its decision. It may reject the request if the request does not amount to one for the request for the correction or deletion of data. Where the agency determines to correct or delete the data it shall do so within 7days and inform the data subject within 7 days from the date of the action.

The broader provisions of the Task Force Bill should be retained as well as specific timelines as provided for in the Senate Bill, within when action under these rights should be taken.
The right to 'erasure'/ right to be forgotten should be provided for clearly and separately from the right to correction or rectification.

Where an Agency may not Notify

Under the Task force bill, the notification of a breach of security of personal data is not required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data (s. 38 (6))

Under the Senate Bill an agency is not required to notify if it has prior to collecting the information taken those steps in the recent past when collecting the same information or information of the same kind from that data subject (s.11(1)). However where this information is to be used for a different purpose from the one for which the information was first collected or where the circumstances of the data subject has changed the agency is to notify data subject of the use to which the information shall be put*(s.11(1))*.

Under the Task Force Bill 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 communicate to the data subject*, unless the identity of the data subject cannot be established (s. 38(1)(b)*

Unless the complete extent of breach can be determined s. 38 of the Task Force Bill should not apply considering the short timelines that ought to be considered between breach and notification of a data subject and the relevant authority.

10. Limitation to Retention of Information

In both Bills (s. 35 of the Task Force Bill and s. 19) of the Senate Bill a data controller/ data processor/agency may retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is —

- required or authorised by law;
- reasonably necessary for a lawful purpose;
- authorised or consented by the data subject; or
- for historical, statistical or research purposes

The Senate Bill uniquely allows an agency to retain data for a longer period than is provided under any law or necessary to achieve the purposes for which the data was collected if the retention is required by virtue of a contract between the parties to the contract.

The Senate Bill further provides that an agency that retains data for historical, statistics or research purposes shall *ensure that personal data is protected against access or use for unauthorised purposes.*

The Task Force Bill requires the data controller/processor to delete, erase, anonymise or pseudonymise personal data not necessary to be retained in a manner as may be specified at the expiry of the retention period (s.35 (2) while the Senate Bill requires an agency, at

the expiry of the retention period, to destroy or delete personal data in a manner that prevents its deconstruction in an intelligible form (s. 19(4).

There are insufficient remedies to threats, violations, and infringements of the rights of data subjects even though their rights are provided for under the Bills. In this instance, for example, the Bills would hardly provide a remedy for exposure of data that ought to (after such a request was made by the data subject) have been deleted.

11. Lawful Processing of Personal Information

The Bills conceptualize lawful processing in different ways.

The Task Force Bill (s. 27) has the same standard for lawful processing as the GDPR and requires consent from the data subject before processing is done for specified purposes necessary for performance of a contract, compliance with legal obligations, to protect vital interests of the data subject, for performance of a task carried out in the public interest, for performance of a task carried out by a public authority or functions of a public nature, for legitimate interests pursued by the data controller, processor or third party to whom the data is disclosed and for historical, statistical and scientific research purposes.

The Senate Bill (s.14) requires that the data be processed in a lawful and reasonable manner and without infringing on the data subject's or other person's right to privacy. The data subject is accorded the right to information relating to the processing of the data, place of origin of the data, use to which the data collected will be put to, information regarding any other person to whom the data will be transmitted, rectification of incorrect data and deletion of data processed without the consent of the data subject.

12. Personal Data Relating to Children

Both Bills provide for parental consent prior to collection of data**.**

The Taskforce B ill however, uniquely requires the data controller or processor to process data in a manner that protects and advances the rights and best interests of the child (s. 29(1)) and to provide for mechanisms for age verification (s. 29(2)) in order to process personal data determined by volume of personal data (s. 29(2)(a)) processed, proportion of that data to be that of children(s. 29(2)(b)) and the possibility of harm to children arising from that processing(s. 29(2)(c)). This is not contemplated in the Senate Bill.

The Senate Bill uniquely requires processing of personal data relating to children be necessary to comply with the law (s. 29(b), for research and statistical purposes (s. 29(c) and be publicly available (s. 29(d).

The authority should be able to specifically address children on the risks, rules, safeguards and rights in relation to processing activities that are addressed at them. Information where processing is addressed to a child should be in a clear and plain language that a child can easily understand.
Children should not be subjected to automated processing.

13. Processing Sensitive/Special Personal Data

This category of information is referred to as *'Sensitive'* personal information in the Task Force Bill (s.2) and as *'Special'* Personal Information in the Senate Bill (s2).

Both Bills include information about race, health status, ethnic social origin, political opinion, biometrics in this category.

The Task Force Bill particularly includes belief, personal preferences location, genetic data, sex life, sexual orientation, and personal financial expenditures as 'Sensitive' personal information. These are not included in the Senate Bill.

The Senate Bill includes religious or philosophical beliefs, trade union membership and any information about a data subject relating to the alleged commission of an offence or any proceedings in respect of any offence allegedly committed by a data subject as 'special' personal information. This is not in the Task Force Bill.

The provisions of the legislation should merge the content of 'Sensitive' personal data under the Task Force Bill and the content of 'Special' personal data under the Senate Bill.

Grounds for Processing Special/Sensitive Personal Data

The Bills provide different conditions under which sensitive/special personal data may be processed.

According to the Senate Bill (s.24) an agency may process special personal information where it is carried out with the consent of the data subject, required under national or international law, for the purpose of statistical or research purposes or is publicly available.

These differ from the provisions of processing of sensitive personal information under the Task Force Bill (s. 40) which are that the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to

persons who have regular contact with it in connection with its purposes; and the personal data is not disclosed outside that body without the consent of the data subject.

Processing of sensitive personal data may be carried out where it relates to personal data which is manifestly made public by the data subject or it is necessary for the establishment, exercise or defence of a legal claim, for carrying out the obligations and exercising specific rights of the controller or of the data subject; or for protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

The Data Protection commissioner under the Task Force Bill s. 43(1) has powers to prescribe further categories of sensitive personal data and any further grounds on which those specified categories may be processed with regard to (s.43 (2)):

(a) the risk of significant harm that may be caused to a data subject by the processing of such category of personal data;
(b) the expectation of confidentiality attached to such category of personal data;
(c) whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and
(d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

This is not contemplated in the Senate Bill.

The provision that processing of sensitive personal data may be carried out where it relates to personal data which is manifestly made public by the data subject could easily prejudice the data subject.

Health data

While inferences can be drawn as to the entities that may process health data for purposes provided for under the Task Force Bill (s. 41), the Senate Bill (s. 28) makes specific provisions for insurance companies or medical schemes, schools, administrative bodies, pension funds, employers, and public or private bodies under a lawful duty to manage the welfare of the data subject.

(Some insurance companies collect sensitive/special personal information including finger prints of beneficiaries to an insurance scheme through the hospital before services can be provided)

- **Processing of data concerning health for reasons of public interest should**

not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

14. Restrictions on Processing

The Task Force Bill provides the following restrictions for processing of personal data where (s. 30):

(a) *accuracy of the personal data is contested* by the data subject, for a period enabling the data controller to verify the accuracy of the data;
(b) personal data is *no longer required for the purpose of the processing, but the data subject requires the personal data for the establishment, exercise or defence of a legal claim;*
(c) processing is *unlawful* and the *data subject opposes the erasure of the personal data and requests the restriction* of their use instead; or
(d) *data subject has objected* to the processing, pending verification as to whether the legitimate grounds of the data controller or data processor override those of the data subject.

(2) Where processing of personal data is restricted under this section (s. 30(2)–
(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 defence of a legal claim, the protection of the rights of another person or for reasons of public interest*; and
(b) the data controller shall inform the data subject before withdrawing the restriction on processing of the personal data.

(3) The data controller or data processor shall implement mechanisms to ensure that *time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, is observed.*

The Senate bill restricts processing of **special** information unless
(a) carried out with the consent of the data subject;
(b) required under national or international law;
(c) for the purpose of statistical or research purposes; or
(d) publicly available

The Senate Bill does not have an equivalent clause on restriction on processing of personal data but restricts the processing of special personal data (referred to as 'sensitive' in the Task Force Bill). The Task Force Bill therefore provides restrictions on processing of both personal and sensitive personal data.

15. Processing for Direct Marketing and Commercial Use of Data

Prior consent is a requirement before personal data is processed for direct marketing (s. 33(1) Task Force Bill) or used for commercial purposes (s. 21 Senate Bill).

The Task Force Bill allows the data subject to object to processing of their personal data which includes profiling to the extent related to direct marketing (s.33(2))and where this is done, the personal data shall no longer be processed for that purpose(s.33(3)).

The Senate Bill allows use of personal data for commercial use where a person is authorised to do so under a written law and the data subject has been informed of such use at the time of collection of the data (s. 21(b)).

The data subject should have the right to object at any time to the processing of personal data concerning him or her for direct marketing or for commercial purposes.

The right should be made known to the data subject and presented clearly and separately from any other information.

16. Trans Border Flow of Personal Data

Both Bills require that consent be given by the data subject prior to transfer and that there be safeguards with respect to the security and protection of the personal data at the place of transfer (Task Force Bill (s. 45), the Senate Bill (s. 31) and must be necessary for the performance or conclusion of a contract and for the benefit of the data subject.

Both Bills require that the transfer be:

a) necessary for the performance or conclusion of a contract between the data controller, data processor, agency and the third party, other person (s. 31 (c) of the Senate Bill, s. 45(1((c)(i), s. 45(1((c)(ii) of the Task Force Bill) and
b) for the benefit of the data subject (s. 31 (d) of the Senate Bill, s. 45(1((c) (iii) of the Task force Bill).

The Task Force Bill provides a further requirement that consent be given after the data subject has been informed of the possible risks of the transfer such as the absence of appropriate security safeguards.

Unique to the Task Force Bill are the requirements that the transfer be necessary:

a) for any matter of public interest, for the establishment, exercise or defence of a legal claim (s. 45(1)(c)(iii),
b) 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(s. 45(1)(c)(v), or

c) for 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 the data subjects(s. 45(1)(c)(iii).

17. Exemptions

Both Bills (Task Force Bill (s. 47), the Senate Bill (s. 12)) exempt compliance with data protection principles for information necessary to avoid a threat to the maintenance of law and order by any public entity, including the prevention, detection, investigation, prosecution and punishment of an offence or information for statistical or research purposes.

Peculiar to the Senate Bill, an agency is not deemed to have collected personal data if the information collected is publicly available, the data subject authorized collection of the data from a third party, noncompliance does not prejudice the interests of the data subject and noncompliance is necessary for the enforcement of a law imposing a pecuniary penalty, is necessary for the protection of public revenue and property, the institution of proceedings or the conduct of proceedings that have been instituted before any Court, tribunal or the Commission, or for the purpose of an exemption asset out in the law relating to access to information.

An agency is not deemed to have collected personal data if compliance would prejudice the purposes for which the information is collected; compliance is not reasonably practicable in the circumstances of the particular case; the information was not to be used in a manner which resulted in the identification of the data subject; or was used for statistical or research purposes and shall not be published in a form that could reasonably be expected to result in the identification of the data subject and the information is collected pursuant to an authority granted therein or in any other written law

Peculiar to the Task Force Bill, the processing of personal data is exempt if it is for *the assessment or collection of a tax or duty or an imposition of a similar nature (s. 47(2) (e)).*

The rights of the data subject in the Task Force Bill are taken away by s. 47(3) which provides that a certificate signed by the Cabinet secretary is sufficient evidence of exemption as necessary for national security and public order and s. 50 which provides that the Cabinet Secretary may prescribe other instances where compliance with certain provisions of this Act may be exempted. The legislation needs to provide specific circumstances for exemptions, as well as for rights that should not be limited, such as the right to correct information that is incorrect.

18. Regulations

The Senate Bill provides that the Cabinet Secretary may make regulations in consultation with the Commission (s.39 (1)) while in the Task Force Bill, this power is only given to the Cabinet Secretary (s. 61).

The Task Force Bill uniquely gives the Cabinet Secretary power to make regulations concerning:

a) requirements to be imposed on data controllers and data processors (s. 61(a),
b) contents for the notice or registration by them (s. 61(b),
c) charges and fees (s. 61(d), issuing and approval of codes and guidelines (s. 61(e), and
d) any other information the Cabinet Secretary may deem fit (s. 61(f).

The Senate Bill on the other hand gives the Cabinet Secretary power to make regulations on the:

a) making of applications (s. 39(2) (a),
b) procedure for and service of notices and documents (s. 39(2) (c), and
c) forms necessary to effect implementation and administration (s. 39(2) (d).

The Senate Bill limits the powers of the Cabinet Secretary to bringing into effect its provisions, the fulfillment of the objectives specified under it and the principles and standards set out under the Interpretation and General Provisions Act and the Statutory Instruments Act, 2013 in relation to subsidiary legislation (s. 39(3).

The authority should be able to issue opinions on issues related to data protection to parliament and other relevant bodies due to its unique position to monitor developments that impact the protection of personal data such as the information and communication technologies and other commercial practices.

19. Consent

The Task Force Bill provides a blanket provision for determining whether consent was freely given in 28(c) and rather than go into detail it makes provision in policy terms.

- **There are no provisions for consent given for multiple purposes, and where this is the case, to be given for each purpose.**
- **There are no provisions regarding silence, pre-ticked boxes or inactivity and whether they would or would not constitute consent.**
- **There are no provisions on what should constitute a request by electronic means.**
- **There are no instances where consent should not be presumed to be freely given. The GDPR, for example, views Consent as not freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment, especially where public authorities are concerned.**
- **Processing of data concerning health for reasons of public interest should**

not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

- **While considering s. 28 (3) of the Task Force Bill, Consent in the GDPR is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.**
- **The legislation should be able to provide for these circumstances.**

20. Data Controllers

A "Data controller" in the Task Force Bill 'means a natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purpose and means of processing* of personal data' while in the Senate Bill a "data controller" is 'a person who, either alone or together with other persons, *controls the contents and use* of personal information'.

In the Task Force Bill there is a "data processor" who is '*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller*' while the Senate Bill contemplates an "agency" who is '*a person who collects or processes personal data'*.

According to the Task Force Bill, all data controllers must be registered with the Data Commissioner (s.15). This requirement is not there in the Senate Bill for any Data Controller or agency.

The application for registration under the Task Force Bill is to include (s.16 (2)):

(a) a *description of the personal data to be processed by the data controller or data processor, and of the category of data subjects, to which the personal data relates*;
(b) a statement as to whether the data controller or data processor is *likely to hold any categories of sensitive personal data*;
(c) a description of the *purpose* for which the personal data is to be processed;
(d) a description *of any recipient to whom the data controller or data processor intends or may intend to disclose the personal data;*
(e) 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*;
(f) statement as to a representative for the purposes of this Act and details of such representative;
(g) a general description of *the risks, safeguards, security measures and mechanisms to ensure the protection of personal data;* and
(h) any other details as may be prescribed by the Data Commissioner

Where there are any changes to the content as outlined above the data controller or data processor must to notify the Data Commissioner of the change (s.16(5)).

The registration certificate issued thereafter is valid for 3 years (s.17).

The Task force bill also provides for a 'Data Protection Officer' appointed on conditions determined by the data controller or data processor where (s. 21) —

(a) *the processing is carried out by a public body or private body*, except for courts acting in their judicial capacity;
(b) the *core activities* of the data controller or data processor consist of processing operations which, by virtue of their *nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale*; or
(c) the core activities of the data controller or the data processor consist of *processing on a large scale of sensitive categories of personal data.*

(2) A data protection officer may be a staff member of the data controller or data processor and *may fulfill other tasks and duties provided* that any such tasks and *duties do not result in a conflict of interest.*
(3) A group of entities may appoint a *single data protection officer* provided that such officer is easily accessible by each entity.
(4) Where a data controller or a data processor is a public body, *a single data protection officer may be designated for several such public bodies, taking into account their organisational structures*.
(5) A person may be designated or appointed as a data protection officer, if that person has *relevant academic or professional qualifications* which may include knowledge and technical skills in matters relating to data protection.
(6) *A data controller or data processor shall publish the contact details of the data protection officer and communicate them to the Data Commissioner.*

(7) The **responsibility of a data protection officer** under the Task Force Bill is to —

(a) *advise* the data controller or data processor and their employees on *data processing requirements provided under this Act or any other written law*;
(b) ensure on behalf of the data controller or data processor that this Act is *complied* with;
(c) *facilitate capacity building* of staff involved in data processing operations;
(d) provide *advice on data protection impact assessment*; and
(e) *Cooperate* with the Data Commissioner and any other authority on matters relating to data protection.

The requirement for registration of data controllers is likely to prove problematic as it encompasses a wide array of persons.
It is likely to be punitive to SMEs due to its licence requirements.
Proposal:

- **Categorize the kind of entities, either by size, or volume, and sensitivity of data (as in the GDPR) handled for registration.**
- **The other obligations of a data controller would continue to apply to SMEs.**

21. Enforcement and Oversight

Under the Task Force Bill implementation and enforcement is to be overseen by the *Data Protection Commissioner* (s. 7(1) (a)) while under the Senate Bill implementation and enforcement is to be overseen by the Kenya National Commission on Human Rights (s. 32).

Under the Task Force Bill Implementation and enforcement is to be overseen by the *Data Protection Commissioner* (s.7 (1) (a)) while under the Senate Bill implementation and enforcement is to be overseen by the Kenya National Commission on Human Rights (s. 32).

The **similarities** in the functions of the Data Protection Commissioner and the Commission overlap in their roles to receive and investigate any complaint by any person on infringements of the rights provided for in the bills. (S. 7(1) (e) of the task force bill and s. 33(1) (d) of the Senate bill).

Whereas the Data Protection Commissioner is to ensure the country's compliance on data protection obligations under international conventions (s. 7 (1) (h)), the Commission under the Senate Bill is to have regard to the applicable international information management and dissemination standards relating to data protection while performing its functions (s. 33(2)(b).

The Senate Bill requires the Commission to ensure that agencies have put in place adequate safeguards for the protection of personal data (s. 33(2)(c) and the Task Force Bill requires the Data Protection Commissioner to carry out inspections of public and private entities with a view to evaluating the processing of personal data 7(1)(g) and to exercise control on all data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act (s. 7(1)(c).

Other functions of the Data Protection Commissioner under the Task Force Bill (s.7) include to:

a) oversee implementation of the Act and be responsible for its enactment;

b) establish and maintain a Register of data controllers and data processors;
c) exercise control on all data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;
d) promote self-regulation among data controllers and data processors;
e) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;

f) carry out inspections of public and private entities with a view to evaluating the processing of personal data;
g) ensure country's compliance on data protection obligations under international conventions;
h) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals;
i) perform such other functions as may be prescribed by any other law or as considered necessary for the promotion of object of this Act.

The powers of the Commission under the Senate Bill (s. 33) include to:

a) promote the protection and observance of the right to privacy;
b) *monitor, investigate and report on the observance* of the right to privacy;
c) formulate, implement and *oversee programmes intended to raise public awareness* of the right to privacy and obligations;
d) receive and investigate any complaint relating to infringement of the rights of a person under this Act;
e) provide a framework or mechanism for the effective management of conflicts and the resolution of disputes under this Act; and
f) perform such other functions as may be prescribed by any other law or as the Commission may consider necessary for the promotion and protection of human rights.

Particular to the Senate bill (s. 33(2)), the Commission is also to:

(a) be guided by the national values and principles of governance under Article 10 of the Constitution;
(b) ensure that agencies have put in place adequate safeguards for the protection of personal data;
(c) ensure that agencies have put in place adequate safeguards for the protection of personal data;
(d) take statements under oath in relation to any investigation it is undertaking; and
(e) take such action as may be necessary for the performance of its functions under the Act.

Where the Data Protection Commissioner under the Task Force Bill is appointed by the Cabinet Secretary, the constitution of the commission under the Kenya National Commission of Human Rights is appointed by a panel consisting of persons representing diverse interests and organizations. (s. 11 Kenya National Commission on Human Rights Act)

The powers of the authority could be expanded to :

a) Issue warnings and reprimands where operations are likely to or have infringed the rights of the data subjects;
b) Impose a temporary or definitive limitation including a ban on processing;
c) Order the suspension of data flows to a recipient in a different jurisdiction or

an international organization;

d) Order communication of breach to a data subject;

e) Order a data controller, processor or agent to comply with the request of the data subject exercising a right;

f) Advise the government, and other bodies and institutions on administrative and legislative matters related to data protection;

g) Cooperate with like authorities in other countries to provide mutual assistance beyond ensuring compliance with international best practice;

h) Monitor developments to the extent that they impact the protection of personal data in the development of information and communication technologies; and

i) Representation by qualified representatives should be allowed for the data subjects before the authority.

22. Data Portability

This right is only provided for in the Task Force Bill in the following terms, similar to the GDPR:

> **34.** (1) 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.
>
> (2) A data subject has the right to transmit the data obtained under subsection (1), to another data controller or data processor without any hindrance.
>
> (3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.
>
> (4) The right under this section shall not apply in circumstances where—
> (a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or
> (b) it may adversely affect the rights and freedoms of others.
>
> (5) A data controller or data processor shall comply with data portability requests, free of charge and within a period of one month.
>
> (6) The period under subsection (5) may be extended for a further two months where data portability requests are complex or numerous.

The Task Force Bill goes a step further than the GDPR to include a specific time line (one month) under which a controller should comply with a request for data portability s. 38 (5) which can be extended depending on complexity or number of requests.

The Task force Bill adequately provides for data portability. This right should be included in the final piece of legislation.

23. Offences

Similar offences in both Bills include making false and misleading statements to the authority and failing to comply with notices issued by the authority in exercise of its mandate.

Unique to the Task Force Bill are offences such as:

- Failing to notify the data commissioner of changes in particulars in the application for registration (s.16 (7)).
- Contravening the provisions governing processing of Sensitive Personal data under Part V of the Bill (s. 42).
- Unlawfully disclosing personal, data in a manner incompatible with its purpose, without lawful excuse on the part of a data controller (s.58 (1)).
- Unlawfully disclosing personal data without prior authority of a data controller, on the part of a data processor (s.58 (2).
- Obtaining access to, or obtaining any information constituting data without prior authority of a data controller or data processor (s.58 (3)).
- Offering to sell personal data where such personal data has been obtained contrary to s. 58(1) (s. 58(5).

Unique to the Senate Bill are offences such as:

- Interfering with personal data of a data subject or infringing on the right of a person to privacy (s.23).
- Collecting or processing personal data in any manner contrary to the provisions of the Act (s.38 (1)).
- obstructing, hindering or preventing the Commission or any other person from the performance of their functions (s. 38(2) (a)).
- holding out as having Authority to perform any action or exercise any powers under the Act while without any authority to do s (s. 38(2) (c)).

Penalties under the Bills differ. The maximum penalty under the Task Force Bill is a fine not exceeding five million or an imprisonment term not exceeding 5 years or both. Under the Senate Bill, is a fine not exceeding five hundred thousand shillings or to a term of imprisonment not exceeding five years, or to both. However where the offence is failing to comply with a notice issued under the Act, one is subject to a fine not exceeding one hundred thousand shillings or to a term of imprisonment not exceeding two years, or to both.

Neither of the Bills provide for compensation for data subjects whose rights have been threatened, infringed or violated. This needs to be provided for as the purpose of a Data Protection legislation is to protect the data subject and provide for remedies where such protection is not upheld.

24. Automated Decision Making

Both Bills prohibit subjecting data subjects to decisions based solely on automated processing which produces legal effects concerning or significantly affecting the data subject. (s. 31(1) of the Task Force Bill and s. 13(1) of the Senate Bill.

The Senate Bill particularly allows for automated processing where the processing of data was necessary to avoid a threat to the maintenance of law and order by any public entity, including the prevention, detection, investigation, prosecution and punishment of a crime.

The Task Force Bill allows for automated processing where the decision is:

a) necessary for entering into, or performing, a contract between the data subject and a data controller;
b) authorised by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
c) based on the data subject's explicit consent.

The Task Force Bill prohibits any automated processing of personal data intended to evaluate certain personal aspects relating to an individual *based on sensitive categories of personal data*.

25. Other Issues

1. **The freedom of expression and information should be balanced with the right of protection of personal data.**
2. **The broad exemptions for public entities in both Bills will likely give rise to abuse. There is hardly any protection accorded to data subjects therefore, from violations, threats or infringement of rights by public bodies.**
3. **The Authority should be able to perform tasks and exercise its powers free from external influence, whether direct or indirect and should neither seek nor take instructions from anybody.**
4. **Members of the Authority/the Authority should not engage in any incompatible occupation whether gainful or not.**
5. **The data subject should be able to access services from the Authority free of**

charge save for where the services are manifestly unfounded or excessive because of their repetitive nature.

6. **The Authority should be able to encourage data controllers to develop interoperable formats to enable data portability.**
7. **The Bills do not provide for any standards to data processed outside Kenya beyond requiring existence of data protection laws for data transfer. The personal data of Kenyan citizens processed elsewhere is still at risk in this regard.**
8. **There are hardly any standards that security and law enforcement agencies are held to, in both Bills, with regard to processing of personal and sensitive/special personal data. There should be judicial oversight for gathering and use of information for threats to maintenance of law. At the rate at which personal information and sensitive/special personal information is being collected, a surveillance state just might be our reality.**
9. **The Authority should encourage innovation grounded on protection of personal data in order to reap the full benefits of big data without trading off privacy.**

26. Conclusion

There is need for a Data Protection Act in Kenya that effects Article 31(c) and (d) of the Constitution. There can only be one Act. It would be prudent to merge the strengths of both Bills and work on their weaknesses in order to have one Act of Parliament to effect the rights accorded in the Constitution.

For any comments, questions or further enquiries, kindly reach me on njokiluc@gmail.com

Njoki Mwangi.