Section	Issue	Summary	Request	Rationale	GDPR Equivalent Language
Clause 4	Ambiguous scope	The scope of the legislation is unclear as it could be taken to refer to any entity with processing activities occurring in Kenya	Clarify to refer to entities incorporated in or with their primary place of business in Kenya	The current framing is ambiguous and could create uncertainties regarding who the legislation would cover	
Clause 6.1.5	The right to object decisions solely based on automated processing.. which produces legal effects ..	A very welcome protection against “AI” injustices.			
Clause 6.1.6	The right to complain	The “right to complain” is and of itself is redundant	Provide for a mandatory complaints handling procedure	Fundamental Freedom of Expression guarantees opinions	
Clause 6.1.9	Creates an unqualified right to be forgotten (right to erasure)	This right needs to be balanced against the freedom of information and the public interest	Clarify the designation of this right as the right to erasure, rather than the right to be forgotten State clearly that the right to erasure is not	The term 'right to be forgotten" is a nebulous term that implies an action (being forgotten) that is beyond the control of the data controller. The right to erasure would	Article 17 - it recognizes a right to erasure (not the right to be forgotten) in certain circumstances; -The purpose for which the personal data has been exhausted and the data is no

			absolute or unlimited. Define the circumstances when the right to erasure applies	violate other basic rights if it was applied absolutely. These include the public's right to information and the protection of public interest.	longer necessary or relevant - The data subject withdraws consent and there's no other justification or legitimate interest in continued keeping of the data - The personal data has been unlawfully processed - Erasure is necessary to comply with a legal obligation Exemptions to the right to erasure and reasons to refuse to comply include: - Right of freedom of expression and information -Compliance with legal obligations or authorities - Public interest - Archiving purposes for public interest; scientific and historical research, statistical purposes - Exercise or defense of legal claims
Clause 6.1.13	New Clause	Policy fails to speak to archived data upon subject's permission revocation	Compel data controller to delete all archived personal data	Caters for archived Personal Data upon data subject revoking use consent	
Clause 7.6	Big Data and Analytics	Use of undefined, composite terms	Propose: "the capture, storage, analysis, search, sharing, transfer, visualization, querying, updating,	"Big Data" and "Analytics" mean different things to different people. Need to avoid technical lingo for more policy clarity	

			and or related other control or processing of complex data and data sources"		
Clause 8.6.2	Negates the Title of Section	The Data Controller may disapprove a request but must provide reasons for denying access to the Data Subject.	Under no circumstances can a data controller (a) be permitted to decline request and (b) and add must provide it within a reasonable time	Clause Negates the Title provision (re: "**Data controller shall uphold rights of data subject"**) – i.e. it erodes data subject's right)	
Clause 9.1	Office of the Data Protection Regulator	ODPR bullets lacks a clear a provision to directly receive data subject's complaints.	Change bullet no. 2 to"**Receiving complaints on any personal data violation**"	ODPR Responsible for upholding the Bill of Rights and enforcing the application of Article 31 of the Constitution on the protection of Right to Privacy	
Clause 12.1	Implementation	Phraseology and procedural	The gradual implementation of this policy, law and regulation will involved (i) policy validation and approved. (ii) Enactment of the *Privacy and Data Protection Bill, inter alia,* establishing "Office of Data Protection Regulator" and finally Regulations governing law implementation.	In its current form the Policy clause seek to create an Office best established by law. The clause also seems to forget (Policy→Law→Regulations) chronological Standard Operating Procedure.(Grammar notwithstanding….)	
Appendix A:	Definition of Anonymisation	refers to undefined "information"	Appendix A to include definitions of "information" and "personal information"		

			consistent with Access to Information Act (No.31) of 2016 ["**information"** includes all records held by a public entity or a private body, regardless of the form in which the information is stored, its source or the date of production; **"personal information"** means information about an identifiable individual, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical, psychological or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual; (b) information relating to the education or the medical, criminal or employment history of		

			the individual or information relating to financial transactions in which the individual has been involved; (c) any identifying number, symbol or other particular assigned to the individual; (d) the fingerprints, blood type, address, telephone or other contact details of the individual; (e) a person's opinion or views over another person; (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) any information given in support or in		

			relation to an award or grant proposed to be given to another person; (h) contact details of an individual.		
Appendix A:	Definition of of Office of the Data Protection Regulator	Office of the Data Protection Regulator / Supervisory authority	Office of the Data Protection Regulator (“Supervisory Authority”) An independent public authority established by **law** to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance.	Reinforce legal certainty on the establishment of the Regulator’s Office.	
Appendix A:	Definition of Personal Data	Definition of Personal data is exclusivity and or circular-referencing	Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.	To cross reference with prior defined “information” and “personal information”	

Appendix A.	Sensitive personal data (m)	Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	Delete clause	Court records are public documents core to access to Information Act. In any case, policy should declare whether proposes the repeal of the National Council for Law Reporting Act (NO. 11),1994.	
Bill Part III 16-20	Registration with DPO	The proposed legislation requires registration of data processors and controllers in Kenya with the Data Protection Officer including the requirement to document and keep up to date a record of processing activities. The bill contemplates the potential requirement of fees for processors to register with the state and penalties for failure to register.	1. Strike requirement for data processors and controllers to register with the Data Protection Office entirely. 2. Note Creative/Artistic Freedom Guaranteed by transition from “License Require to innovate” legacy legislative routes. 3. Avoid creating new obstacles to local tech innovation 4. Avoid creating yet another “Revenue Authority”	Data Processing and Data Controlling are not business models in the strict sense. They are activities that entities may incidentally engage in during the course of business. The requirement to have all processors and controllers would create an immense implementation burden for the Data Protection Office that would threaten to bog down the office with bureaucratic recordkeeping rather than allowing them to focus on the most serious enforcement issues. Similarly, for processors and controllers, the requirement to update external records of	N/A no parallel requirement for registration in GDPR

				processing each time a change to processing occurs shifts the focus from improving privacy in areas that present the most risk to a bureaucratic exercise. The requirement for fees also raises issues as this would disproportionately affect smaller data processors and controllers.	
Policy Clause 5.5.1; Bill section 23(c)	Accuracy	Accuracy requirements appear to create a positive obligation to keep data that is accurate and up-to-date.	Strike affirmative requirements for accurate and complete data	As a right to rectification also exists in the legislation controllers and processors will still be required to take steps to update data where it is identified by the data subject as either inaccurate or incomplete. This is the correct framing as absent notification by the subject controllers and processors may be unaware of whether data is complete and accurate without undertaking further processing.	Article 16 - Right to Rectification The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Bill section 25	Insert new Subsection 25(4)	Whereas section 25(2) (f) good intention of crime prevention, incomplete false and misleading information collected for other purposes (thus arguably "illegally collected evidence") violates privacy, fair administration of justice, among other fundamental rights. However noble the intent but null to the extent of conflict with the Constitution.	Considering the plausibility of personal data being incomplete, inaccurate, false and or misleading, a data controller or data processor shall not tender any such collected personal data under subsection (3) in legal proceedings as evidence detrimental to the interests of the data subject.	To balance fundamental individual rights guaranteed by the Constitution against surveillance state machinery	
Bill Section 36(a)	Erasure	Does not clarify that the right to erasure is based on areas where the processing is based on content and such consent has been revoked	Clarify that erasure rights are associated with where processing is occurring on the basis of consent	In cases where the processing is not based on consent the legitimate interest may persist even after consent of the individual has been revoked if that interest persists and continues to justify processing	Article 17 - Right to erasure ('right to be forgotten') 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the

					processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
Policy Clause 7.3.1; Bill Section 23 (1)(b)	Consent	Though the bill allows for processing in circumstances where consent has not been provided (legitimate basis, historical/scientific research, etc.) non-consent based processing is referred to as an exceptional circumstance	All of the permissible bases for processing should be framed as equally good options for justifying processing rather than as fall back where consent cannot be obtained	All bases set forth within the proposed legislation should be treated as equivalent under the law	Article 6 - Lawfulness of processing 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of

					his or her personal data for one or more specific purposes; (b) 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; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) 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; (f) 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.
Bill Part VI (Section 46-47)	Cross-Border Transfer	The proposed legislation bars transfer of data to a third country where there is no decision by the Data Commissioner that adequates safeguards have been made for the protection of that data (adequacy decision). The omission of the word 'or' at the end of the conditions listed in this part gives the interpretation that all of those conditions listed have to be met before data can be transfer across borders. IT appears that this may not have been the intention and that all the conditions listed are mutually exclusive.	Permit transfers to third country where, accounting for the transfer, all of the other requirements set forth in the legislation will continue to be met. Clarify that the conditions listed in part VI are mutually exclusive. Do this by using the term "...may transfer personal data to another country **where any of the following conditions is fulfilled"** or separate the conditions with the term 'or'.	Requirement for adequacy decision will have undesirable impact on restricting free-flow of data. Concerns may be addressed through alternatives like binding corporate rules, codes of conduct, and certifications.	Article 49 - Derogations for specific situations 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-

					contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest; (e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order 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; (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent

					that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection

					of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.
Policy Clause 8.5; Bill section 38(1)	Notification of breach	The proposed legislation requires notification to the Data Protection Officer for all instances of breach and not just those that are likely to have an impact on the rights of the data subject.	Revise to require notification only where breach is likely to result in a risk to the rights and freedoms of natural persons	As currently drafted could have risk of inundating Data Protection Office with notices for risks that are trivial in terms of impact on rights of individuals. A more efficient and effective means to enforcement would come from narrowing notification to those breaches likely to have an impact on individual rights and freedoms	Article 33 - Notification of a personal data breach to the supervisory authority 1. 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. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
Policy clause 8.3.3	Pseudonymization	The proposed legislation states that even where	Pseudonymised data should only be treated	Current framing disincentivizes use of pseudonymization	(26) The principles of data protection should apply to any

- Definitions		pseudonymized data is kept separately from data that would make it re-identifiable and measures to ensure it cannot be attributed to an identifiable person, it still falls within the scope of personal data.	as personal data in contexts where it may be attributable to a natural person accounting for the organizational measures described	techniques which, where data is no longer personally identifiable, provide significant improvement in privacy.The current treatment may also create ambiguities in other aspects of the proposed legislation where the data subjects rights cannot be exercised due to the inability to attribute data to a natural person.	information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to

					anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes. Article 4 - Definitions ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
Bill sections 17(7), 40(2), 64(6)	Penalties	The fines set forth in the proposed legislation are not clearly mapped to the	Affirm that the penalties accorded for violations of data protection rules	Lack of clarity on how fines will be applied creates significant ambiguity for processors about	Article 84 - Penalties 1. Member States shall lay down the rules on other

		likelihood or severity of the breach.	should be consummate to the nature, gravity, and extent of the infringement	how penalties will be assessed and could have a chilling effect considering the steep penalties contemplated.	penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.
Bill Part V (sections 40-45)	Sensitive Personal Data	Special personal data may not be processed according to all legitimate bases and exceptions provided are very narrow (e.g. religious and political institutions for their membership) even where other parties may have legitimate interests	Allow processing according to all of the lawful/legitimate bases provided, provided that the unique sensitivity of the data must be accounted for in assessing the processing and necessary safeguards	There may be strong legitimate interests in processing of sensitive data categories that are not provided for by the close-ended list of exceptions. Where data controllers are accounting for the nature of the data in assessing whether the interests are legitimate and in determining what safeguards are required processing may still be considered lawful.	1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law

					provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its 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 that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary

					for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

					L 119/38 EN Official Journal of the European Union 4.5.2016 (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate. to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
Policy Clauses 5.2.3, 7.1; Bill section 32	Balancing Test	Process for determining whether processor has a legitimate interest in the processing is unclear, references are only called out in the context of objection to processing	Articulate balancing test wherein processing may be considered legitimate if the controller's interest in processing outweighs impact on rights and freedom of the individual in having his or her data processed	A clearly articulated balancing test will help lessen ambiguity about the specific circumstances in which processing may be considered legitimate based on the interest of the controller.	Article 6 - Lawfulness of processing 1. Processing shall be lawful only if and to the extent that at least one of the following applies: ... (f) 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.