MEMORANDUM ON POLICY AND REGULATORY FRAMEWORK FOR PRIVACY AND DATA PROTECTION, 2018

SUBMITTED BY

THE KENYA ICT ACTION NETWORK (KICTAnet)

TO

THE TASKFORCE ON POLICY AND REGULATORY FRAMEWORK FOR PRIVACY AND DATA PROTECTION IN KENYA

21 SEPTEMBER 2018

CONTENTS

Introduction **1**

Comments on the policy **2**

Matrix on the policy **3**

Comments on the Bill **11**

Matrix on the Bill **12**

Introduction

The Kenya ICT Action Network (KICTANet) is a multistakeholder platform for people and organisations interested in ICT policy reform. KICTANet welcomed the formation of the taskforce on privacy and data protection in Kenya by the Cabinet Secretary, ICT in May 2018. From 21-30 August, the network carried out a moderated online discussion on provisions of the framework published by the taskforce.[1] There was also a forum on the framework that took place at Strathmore University on 23rd August. From these two fora, it emerged that there was need for a session to read the Bill in depth. Accordingly, a focus group discussion with a group of ICT lawyers and practitioners was held on 12 September 2018 at Ngong Hills Hotel. Subsequently, the question of legacy of personal data on demise of the data subject was posted to the online platform for discussion. These submissions were developed from collecting views during these interactions.

Kenya has a growing data economy. In the 2017 elections for instance, public and private institutions required data to better provide services. The Independent Electoral and Boundaries Commission (IEBC) updated the voter register which is a database containing personal details, including biometric data of over 19 million voters. Kenya boasts of 87% connectivity, which means that data of over 40 million subscribers is held by mobile network operators and other service providers. Indeed, during the election period, there was widespread use of data such as voter details and telephone numbers for political mobilisation and campaigning.

The data economy will continue to grow. In less than a year, the government will undertake a nationwide census. The census is carried out once every 10 years and this time round, it is expected that there will be more data collected. In addition, digital technologies will likely be employed in studying the data to understand patterns in population distribution and also predict future scenarios. For example, the data will show where there has been growth in population and predict where there is likely to be a decrease.

[1] Verbatim dicussions can be accessed on the KICTANet list here https://lists.kictanet.or.ke/pipermail/kictanet/2018-August/thread.html

Such data has the potential of improving service delivery by government by taking services where they are most needed. At the same time, technologies applied on data can and have been shown to deepen existing divides among populations, discriminate against certain sectors of the population or exclude others from service delivery. Hence in the 21st Century, privacy involves protecting the person from exposure and harmful use of their personal data on the one hand, and protecting people collectively from the harms of data processing activities on the other.[2] The first objective is often achieved through data privacy laws while the second is in many jurisdictions, still work in progress.

KICTANet appreciates the taskforce's broad approach to the task of developing a framework for Kenya, which has been achieved through proposing a *policy* as well as *Bill*. Our submissions are therefore on both the *Bill*- which we understand will give the immediate legal framework for informational privacy for individuals- and also on the *policy*-which we believe should contain room for longer term issues including the effect of data processing businesses on the Kenyan society.

Comments on the *policy*

KICTANet appreciates the effort put in elaborating Article 31 of the Constitution of Kenya in the policy. It is commendable that under the policy, the government plans to have a law of general application in data processing. We however view policies as the wider framework describing the government's plans or position towards an issue and argue that the policy should be expanded beyond the law to include other tools that are pertinent in ensuring a rights promoting data economy. These include education, skills development, innovation as well as protection of small players in the economy.

A general comment on the policy is that there is need for more **coherence between the policy and proposed law.** For instance, the policy makes provisions on transparency (clause 5.1), purpose limitation (clause 5.2), transparency (clause 5.7), withdrawal of consent (clause 6.1.12),data protection by design and default (clause 8.3) , administrative fines (clause 9.1), monitoring and evaluation (clause

[2]KICTANet (2018) Data Protection in Kenya https://www.kictanet.or.ke/?wpdmpro=data-protection-in-kenya

11) and phased implementation (clause 12). These are however captured minimally or not captured at all in the *Bill.* Conversely, there are substantive rights abrogating provisions in the *Bill* that are not founded on the policy. These include exemption of public offices from the law (clause 4) and general exemptions (clause 47) including the ambiguously worded exemption for assessment of taxes (47(2)(e)).

KICTANet supports the spirit of the framework and views the *policy* and *Bill* as an appropriate response to Kenya's privacy related problems including profiling and unwarranted surveillance. The framework however requires enhancement to provide the highest protection of privacy for Kenyans and also support an innovative rights promoting data economy. We provide matrix of proposals for amendment of the *policy* and *Bill below:*

Matrix on the policy

	Current provision in the policy	**Proposal**	**Justification**
1	2.3 Objectives of the policy	Include as an objective "to inform the development of a privacy promoting data economy through interventions in laws, education, skills development and innovation"	Expand the policy to include other tools for resolving the problem of privacy and data protection. These include education, skills development and innovation in the data economy

	2.3 Objectives of the policy	Include as an objective “to ensure protection and promotion of the right to privacy among all data processors and controllers, including small and medium enterprises ”	To create a basis for interventions aimed at assisting small and medium data processing enterprises to promote the highest standards of privacy
2	2.3 Objectives of the policy	Include as an objective “to provide guidance for balancing the right to privacy with other rights such as freedom of expression and security”	Inevitably, there will be tension between the right of privacy and other rights. The policy should provide the position on the issue as guidance.
3	4. Scope	Clarify whether the policy applies to Kenyan’s data held outside Kenya in the same way GDPR relates to EU citizen’s data	While it may be impossible to enforce the law outside Kenya, having legal protection could be useful for Kenyans in countries without data protection laws
4	5.7 accountability	Include requirement on transparency and accountability of algorithms used	This enhances privacy and puts an obligation on data processors to develop privacy

		in automated processing	protecting technology for data processing
5	6.1 Data subject’s rights	Delete “There may be limitations on data rights of data subject when required by the law or when there are competing rights and therefore would require an assessment based on the facts and circumstances”	The clause should begin by reinforcing rights as opposed to limiting them
6	6.1 Data subject’s rights (limitations)	Add: Data subjects right to privacy may only be limited in accordance with Article 24 of the *Constitution.* Where data subjects rights are limited, the particular aspect of the right that is limited (eg access to data, information on whether data is being processed etc) will be specifically stated. Limitation of rights does not remove application of	Data protection rights are well elaborated to include access, information whether personal data is being processed, objection to processing, protection from decisions made solely through automated processing, data portability, right to be forgotten, withdrawal of consent and security safeguards for personal data. These rights are quite expansive and when limited without specifics, it is disproportionate and does not give effect to Article 31.

		data protection principles.	
7	7.3 Exemptions to consent	Add: Where consent is not expressly obtained, the data processor is under obligation to register such data processing activities and report annually to the Data Protection Commissioner	Provide promotion of privacy where consent is not acquired from the data and require transparency and accountability in such cases Also, enhance the relationship between the DPC and processors
8	7.6 Big data analytics	Add: Analytics of big data will be subject to transparency and accountability of algorithms and other techniques used to analyse the data during the entire life cycle of such techniques	While acknowledging that big data analytics will be a part of the data economy, we could also reimagine an economy based on protection and promotion of privacy from the start
9	7.6 Big data analytics	Add: Platforms are obliged to share big datasets with data processors in Kenya in anonymised form for Research	To encourage innovation and discourage anti-competitive practices of hoarding big data sets

10	8 Obligations in data processing	Include a section on transparency: Data controller: inform data subject and data protection commissioner of any change or update in data processing activities related to their data. Data processor: be transparent in data processing activities including automated ones. Avail algorithms for inspection by data subject or group of data subjects or data protection commissioner	Data processing is ubiquitous and challenging to understand for the public as data is not tangible. The public should be empowered to understand data processing activities through access to automated data processing technologies such as algorithms.

11	8. Obligations in data processing	Include portability: Data controller shall design or procure systems that support the right of portability. This includes systems that support interoperability. Data processors should where possible port data subject's data to requested processor/controller	Reinforce data portability and make it meaningful by easing the burden on a data subject who desires to move from one platform to another
12	9. Institutional framework	Divorce enforcement of the law from the executive and instead link it to Parliament	The executive is a large data processor that will be subject to the law. To avoid conflict of interest and enhance independence, the data protection authority should be independent

13	13. Related policies	Include other laws and policies: ● Statistics policy ● National research policy ● Health information systems ● National identification	Data processing is cross-cutting and interventions apart from law will involve other data heavy sectors such as statistics, research, health informatics and national identification systems.

Comments on the Bill

KICTANet appreciates that the Bill aspires to give effect to informational privacy under Article 31(c) and (d) of the Constitution of Kenya. The inclusion of principles of data protection as well as rights of data subjects will make privacy more meaningful for Kenyans whose data is ever more required in the digitalised world we live in. The law could further be enhanced through:

a) Making **protection and promotion of privacy the default** position in provisions of law. In the limited situations where there is necessity for limitation of the right, the restriction should be narrow and specific to avoid ambiguity that may result in discretionary application of the law hence qualification of the right to privacy. Further, since the different aspects of privacy are described in the Bill, limitations should specify the affected aspect and state that unaffected aspects still apply. For example, should access to personal data be limited for a data subject for reasons of investigation of a crime, this should not take away aspects such as right of the subject to know if data about them is being processed or the right to accuracy and security of the data.

b) Relatedly, the law should be one of **general application**, subjecting all data controllers and processors, including public agencies and government departments to data protection principles. No entity or practices of an entity should be exempted from application of the law. If any exemption is to be allowed, it should be defined in the proposed law and not left to the discretion of the executive. In addition, data protection regime should not be used to enhance operations of public offices and government agencies by giving them access to datasets of registered controllers and processors. The Bill cannot therefore abrogate the right to privacy through blanket exemptions such as those provided for in clause 4 or the general exemptions clause.

c) Relationships between the data protection commissioner (DPC) and actors in the data economy. While the policy envisages a powerful DPC who has meaningful relationships with controllers/processors, subjects as well as other stakeholders, the Bill generally does not translate into these relationships. For instance, the DPC has no powers to collect registration fees to fund the office and sanctions such as administrative fines are not included in the proposed law. But of even more concern is the

independence of the DPC. While the policy aspires for independence, the Bill fails to live up to the task as it anchors the office in the executive, then creates discretionary powers in implementation of the law that are granted to the Cabinet Secretary. In addition, the appointment, financing, reporting and removal of the DPC is linked to the Cabinet Secretary.

d) In all our engagements, we heard from **small and medium enterprises (SMEs**) who, in the advent of the General Data Protection Regulation (GDPR) have had major compliance challenges. Since this framework will be enforced in Kenya, they are concerned that they may be edged out of business as they put their systems in order. Even those who comply fear that they will be edged out of business such as big data analytics which in their view, this framework puts bigger players and multinationals in an easier position of compliance. They therefore sought to have the policy have registration classified according to size of data held and sanctions graduated accordingly. Further the data protection commissioner should design education, awareness, skills and standard development interventions aimed at assisting these players to promote the highest standards of privacy.

Matrix on the Bill

	Clause in the Bill	**Proposal**	**Justification**
1.	**Clause 2: Interpretation** "consent" means any voluntary, specific and informed expression of will of a data subject to process personal data;	"consent" means any **the** voluntary, specific and informed expression of will of a data subject to process personal data;	The use of the word 'any' makes it appear as though consent could be cavalier.
2.	**Clause 3: Object and purpose**	(f) to provide for the limitation of	The right to privacy can only be

	To add:	the right to privacy in specified cases	limited in accordance with Article 24 of the Constitution which requires an unequivocal qualification of when this right will be limited.
3.	**Clause 4(1)(b): Application** To add:	(iii) not established or ordinarily resident in Kenya but processes personal data belonging to Kenyan data subjects	Article 31 protects the rights of Kenyan data subjects without making a distinction of their location. As it is, the section does not bind data controllers and processors who not being located in Kenya process personal data of Kenyan data subjects.
4.	**Clause 4(2)(a): Application** This Act shall not apply to – (a) the exchange of information between government departments and public sector agencies where such exchange is required on a need-to-know basis; (c) Processing of personal data	Delete sub-clause	Data protection extends to the protection of data and reporting obligations. The kind of data held by government departments should be held to even higher standards. It may be reasonable to exempt such data from responsibilities such as consent and disclosure, but not to remove it from the purview of the Act entirely.

	exempted under section Part VII.		
5.	**Clause 5(4): Establishment of the Office** The Office shall ensure reasonable access to its services in all parts of the Republic	The Office shall ensure reasonable access to its services in all counties	This will make controllers, processors and data subjects in counties appreciate data protection.
6.	**Clause 6:** (1) The Data Commissioner shall be appointed by the Cabinet Secretary on a competitive basis and on such terms and conditions as may be specified in the instrument of appointment	Delete sub-clause and replace with: (1) The Commissioner shall be nominated by the Public Service Commission and with the approval of Parliament, appointed by the President.	Clause 5(2) designates the Commissioner as a state officer. The Commissioner’s rank is therefore higher than that of a public servant. Further, the Office of the Commissioner is one that calls for independence. Being appointed by the Cabinet Secretary interferes with this independence. Further data protection is cross-cutting and not only an ICT sector issue
7.	**Clause 8(2):** **Powers of the Data Commissioner** To add:	Power to issue other remedies including administrative fines, compensation orders and stop orders	KICTANet recommends administrative remedies and compensation to data subjects as

			well as additional remedies. Please see below under ‘remedies’.
8.	**Clause 9: Delegation Data Commissioner** **9.** (1) The Data Commissioner may, subject to such conditions as the Data Commissioner may impose, delegate any power conferred under this Act or any other written law to— **(c)** a recognised self-regulatory organisation	· Specify which powers can be delegated and which ones the Commissioner should not delegate. · Qualify what amounts to a recognized self-regulatory organisation	While self-governance is encouraged, the Act should restrict the powers that can be delegated to self-regulatory organizations. This is to avoid instances of industry collusions to the disadvantage of the data subject.
9.	**Clause 10 (b): Vacancy in the Office of the Data Commissioner** The Office of the Data Commissioner shall become vacant, if the Data Commissioner— by notice in writing addressed to the Cabinet Secretary resigns from office	The Office of the Data Commissioner shall become vacant, if the Data Commissioner— by notice in writing addressed to the ~~Cabinet Secretary~~ **President** resigns from office	This follows after the change in the way the Commissioner is appointed.

10.	**Clause 16: Application for re registration** To add:	· Specify time within which the Commissioner should issue a certificate	
11.	**<u>Proposed new clause</u>** **Transitional provisions**	· The date by which data controllers and processors ought to apply for registration	
12.	**<u>Proposed new clause</u>** **reports by the Commissioner**	· Provide for reports on case received and their progress · Provide for annual report on performance of this office to Parliament and the public	As this is an Act that concerns the realisation of a human right, the Commissioner should be required to present annual reports to Parliament and to the public

13.	**Clause 16: Application for registration** Alternative approach	· Not all data controllers and processors should be required to register with the Data Commissioner. · Introduce a tiered system where data controllers and processors who meet certain conditions are required to register. This could be based on the type, quantity and sensitivity of data handled.	Requiring all data controllers to be registered may be cumbersome and impractical.
14.	**Clause 16 (5):** **Application for registration** (4) Where there is a change in any particular outlined under subsection (2), the data controller or data processor shall notify the Data Commissioner of such change in prescribed period.	To add: The Commissioner may refuse the data controller or processor from effecting the changes in particulars, where such changes in particulars would have adverse effect on privacy of data subjects. In the event that the Commissioner refuses to effect a change in particulars, they shall give reasons for refusal in writing, and the	Change of particulars in the register should not merely be to inform the DPC. If there is concern about the effect of the change on the rights of the data subjects, DPC should be able to intervene.

		Commissioner may order the data controller or processor to undertake such action as may be necessary to mitigate the latent harm on data subjects.	
15.	**Clause 21** **Designation of the Data Protection Officer** 21. A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where— (a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;	Delete clause (b) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;	The purpose of the court exception is not understood. Furthermore, the courts process a lot of data which in itself necessitates the designation of a data protection officer.
16.	**Clause 21: Designation of the Data Protection Officer** **Alternative approach**	· Those controllers and processors who must register with the Commissioner	This follows the proposal under Clause 16

		should also appoint a data protection officer. · The chief executive officer of the controller or processor should be designated as the data protection officer where the controller or processor has failed to appoint a data protection officer.	
17.	**Clause 22: Principles of data protection** (1) Every data controller or data processor shall ensure that personal data is– (h) not transferred outside Kenya, unless there is **adequate proof of adequate data protection laws** by the recipient country.	Replace (h) with not transferred outside Kenya, unless the country has a is **adequate proof of adequate data protection laws data protection framework relying on similar data protection principles** by the recipient country.	The adequacy of laws is subjective. The focus should be on the quality of protection rendered in the recipient country.
18.	**Clause 25(2): Collection of personal data**	Delete 25(2)(f)(iv) and (v)	Consent is key. Where legal obligations require the collection of

	(2) Despite subsection (1), personal data may be collected indirectly where— (f) collection of data from another source is necessary- (iv) to comply with an obligation imposed by law; or (v) in the interest of national security		data from an indirect source, the enabling legal provisions provide a procedure for such a collection e.g. a court order. Allowing other government entities to access information gives a route for circumvention of the normal procedures (e.g. access by KRA for tax purposes). National security is too broad an exception. Similarly, laws on security give the legal procedure to accessing information e.g. search warrants and court orders.
19.	**Clause 28: Conditions for consent** To add:	The Commissioner shall issue guidelines on how to obtain effective consent.	Issues such as opt-in, use of simple English in terms and conditions may not adequately be captured by the requirements of the Act. To complement the requirement for express consent, the Commissioner may issue guidelines and practice directions covering various situations and industries.

20.	**Clause 31: Automated individual decision making** (2) Subsection (1) shall not apply where the decision is – (a) necessary for entering into, or performing, a contract between the data subject and a data controller; 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	Delete sub-clause 2	These qualifications have the effect of overriding the prohibition under Clause 31(1).
21.	**Clause 32: Objecting to processing** 32. (1) 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	Alternative approach: Where there is a disagreement between the data subject and data controllers or processors, the Commissioner should intervene and make a decision.	To whom should the data controller or processor demonstrate compelling legitimate grounds? The Commissioner would be the right party to intervene in cases like this where there is a conflict between the data subject and the controller or processor

	subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.		
22	**Clause 38: Notification of breach of security of personal data** (6) The notification of a breach of security of personal data shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data;	Delete clause	If data controller has implemented security safeguards and there is still breach, the privacy of data subjects is still at stake and they deserve to know. Exemption from notification abrogates the right to privacy
23	**New clause** Offence of failure to notify in case of breach	Failure to notify data subjects and DPC of a breach under this section amounts to an offence	This creates incentive to comply

24	**Clause 44(3)** **Rule as to data centers and servants** (2) Cross-border processing of sensitive personal data is prohibited.	Alternative approach: List the types of data that cannot be transferred out of Kenya. 'Sensitive data' too wide a category.	The definition of sensitive data offered in Clause 2 is too wide. It includes financial data. Practically, financial data is transferred across borders as a usual business practice e.g. cloud computing. Further, there is no demonstrable harm in storing financial data outside Kenya. This limitation should only extend to data that touches on Kenya's sovereignty e.g. election, immigration and defence data.
25	**Clause 47(2)** **General Exemptions** (2) The processing of personal data is exempt from the provisions of this Act if— (a) exemption is necessary for national security or public order. (b) disclosure is required by or under any a written	Delete sub-clause	The exceptions anticipated are legal situations. There already exists legal rules governing obtaining of data during these situations e.g. obtaining a court order. To exempt these situations from the applicability of this Act is tantamount to excusing the government (as a data controller and processor) from the obligations in the Act.

	law or by an order of the court (c) the prevention or detection of crime; (d) the apprehension or prosecution of an offender; or (e) the assessment or collection of a tax or duty or an imposition of a similar nature		In addition, the provision seems to be providing an avenue for public offices and government agencies to easily access datasets. This abrogates instead of enhancing privacy.
26	**Clause 47(3)** **General Exemptions** For purpose of subsection (2) (a) a certificate signed by the Cabinet Secretary shall be sufficient evidence of exemption from outlined provisions of this Act.	Delete sub-clause	This interferes with the independence of the Commissioner and creates an opportunity for abuse of power. Good laws should aim for more precision and less discretion.
27	**Clause 49:** **Research, history and statistics** (1) The further processing of personal data for a research	Define and limit research purposes	Any data controller/processor with capacity may change purpose of data on this ground as research can include big data analytics and

	purpose in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained.		market research. This clause abrogates the principle of purpose limitation by giving window for changing purpose
28	**Clause 49:** **Research, history and statistics** (2) Personal data which is processed for research purposes in compliance with the relevant conditions may be kept indefinitely.	Delete clause	Clause abrogates the right to be forgotten as well as the principle of storage limitation directly and data minimisation indirectly
29	**Clause 49:** **Research, history and statistics** (3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if— (a) data is processed in compliance with the relevant conditions; and	Define relevant conditions Add (c) results of the research are made available to the public	

	(b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.		
30	**<u>Proposed new clause</u>** **Research, history and statistics**	Data processors and controllers shall provide datasets in a form which identifies the data subject or any of them to researchers	To encourage innovation and development of products from data as opposed to data silos that are used exclusively by data processors and controllers to stifle competition
31	**Clause 50: Exemptions by the Cabinet Secretary** The Cabinet Secretary may prescribe other instances where compliance with certain provisions of this Act may be exempted.	Delete clause	All the exceptions should be stipulated in the Act. The role of the CS should be relegated to making regulations to expound on these exceptions.
32	**Clause 52(1)(b): Investigation of complaints** **52.** The Data Commissioner may, for the purpose of the investigation of a complaint, order any person to –	Delete the words **which he is not prevented by any other enactment from disclosing;**	The part we propose to strike out undermines the authority of the Commissioner. As a State Officer, he is already bound by rules on confidentiality and fiduciary duties. He should be able to access all the

	(b) produce such book, document, record or article as may be required with respect to any matter relevant to the investigation, **which he is not prevented by any other enactment from disclosing;**		information that could help him arrive at a decision. In any case, appearance of these words in a law gives lawyers an easy way out of production orders by the DPC as they may claim that they are prevented from disclosing any document they are not comfortable doing so
33	**Clause 55(2): Annual estimates** (1) The annual estimates shall be submitted to the Cabinet Secretary for tabling in parliament	Delete sub- Clause	This interferes with the independence of the Commissioner. Like all other independent offices, he should present his budget to the National Assembly.
34	**Clause 57: Annual reports** **To add:**	The Commissioner shall make the annual report public.	For transparency and accountability
35	**Clause 58(1): Unlawful disclosure of personal data** A data controller who, without lawful excuse, discloses personal data in any	Add data processor. Clause to read: A data controller **and processor** who, without lawful excuse,	Should apply to both controllers and processors.

	manner that is incompatible with the purpose for which such data has been collected commits an offence.	discloses personal data in any manner that is incompatible with the purpose for which such data has been collected commits an offence.	
36.	**Clause 60: Codes, guidelines and certification**	Alternative approach: Guidelines and Codes of Practice should be developed by the industry players instead of the Commissioner. Remove the role of the CS to issue regulations governing the certification program.	Industry players are highly specialized and understand their field better than the Commissioner. This also secures their commitment
37.	**Clause 61(f): Regulations** any other matter that the Cabinet Secretary may deem fit	Delete the words "matter that the Cabinet Secretary may deem fit " and replace with any other related matter any other **~~matter that the Cabinet Secretary may deem fit~~ related matter**	Limit the Cabinet Secretary's discretion
38.	**To add:** **Remedies**	1. Administrative fines 2. Compensation for the	These are more effective as compared to criminal penalties

		data subject to be set by the Commissioner 3. Right to sue for civil remedies 4. Account for profits 5. Stop orders and suspension orders 6. Notice to show cause	
39.	**To add:** **Consent**	Under disclosure, the data controller and processor should also be required to inform the data subject of the remedies available in cases the controller or processor is at fault.	
40	**Proposed new clause** **Legacy of personal data**	Provide for legacy of personal data on demise of a data subject. Recomendations include: • when data subject makes a testament on their data in a will, this should be treated as consent • where successors of the data subject or other Kenyans	Although there was no consensus on whether data is property to be inherited, listers were of the view that privacy and dignity are interlinked. On the demise of a person, their dignity should be protected.

		require personal data of the demised to achieve their human rights or in public interest, they should be able to access the data • even where there is no will, dignity of the demised data subject should be protected and sensitive personal data should still be protected • personal data about a demised subject should not be kept indefinitely. Storage limitation should still apply once executors of the estate and other interested parties have used the data	

About KICTANet

The Kenya ICT Action Network (KICTANet) is a multistakeholder space for ICT policy discussions. Founded in 2003, the network acts as a catalyst for reform in the ICT sector in support of the national aim of ICT enabled growth and development. KICTANet has been undertaking policy research with the objective of providing information for people centered decision making in the center. In

2017 the network embarked on an election observation mission to observe deployment of technology in Kenya elections from a user perspective. Among the recommendations from the mission was that Kenya needed to develop a comprehensive data protection framework to protect and promote the right of privacy. More about KICTANet and our work can be found here.

Contact person

Grace Githaiga
Convenor, Kenya ICT Action Network
ggithaiga@kictanet.or.ke info@kictanet.or.ke
@kictanet