PRIVACY INTERNATIONAL

Analysis of Kenya's Data Protection Act, 2019

January 2020

About us

This submission is made by the Defenders Coalition, The Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN), Dr. Robert Muthuri and Privacy International (PI).

Defenders Coalition is a national organization established in 2007 and incorporated in the Republic of Kenya as a Trust in 2012 whose mission is to strengthen the capacity of Human Rights Defenders (HRDs) to work effectively in the country and to reduce their vulnerability to the risk of persecution. The NCHRD-K has a track record in advocating for a favourable legal and policy environment in Kenya, conducting preventive security management trainings and offering support to HRDs at risk through legal, medical and psychosocial support.

Contact: Kamau Ngugi, Executive Director, NCHRD-K, dkngugi@hrdcoalition.org

The Kenya Legal and Ethical Issues Network on HIV and AIDS (KELIN) is an independent Kenyan civil society organization working to protect and promote health related human rights in Kenya. We do this by; Advocating for integration of human rights principles in laws, policies and administrative frameworks; facilitating access to justice in respect to violations of health-related rights; training professionals and communities on rights based approaches and initiating and participating in strategic partnerships to realize the right to health nationally, regionally and globally.

Contact: Allan Maleche, Executive Director, KELIN, Amaleche@kelinkenya.org

Dr. Robert Muthuri is a Legal Knowledge Engineering Consultant. He holds a PhD in Legal Informatics, an LLM in Innovation Technolgy & the Law, and is an Advocate to the High Court of Kenya.

Contact: muthuri.r@gmail.com

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Working internationally through an International Network of partners, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

Contact: Alexandrine Pirlot de Corbion, Director of Strategy, alex@privacyinternational.org

Overview

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 120 countries worldwide including over 20 African countries,[1]and instruments have been introduced by international and regional institutions such as the African Union,[2] the OECD,[3] Council of Europe,[4]and ECOWAS.[5]

We welcome the effort by the Government of Kenya to give life to and specify the right to privacy, already enshrined in Article 31(c) and (d) of the Constitution of Kenya by proposing a draft Data Protection Act. We particularly appreciate the direct reference to this Constitutional right in the purpose of the Act and the way it is referred to on several occasions in the Act.

While these efforts have positive intentions and we are pleased that Kenya has adopted a comprehensive data protection law, the Act adopted has a number of shortcomings which ought to be addressed moving forward with the implementation and application of the Act.

As part of this process, we call on the government of Kenya to review the areas of concerned flagged in this analysis in order to ensure that personal data is effectively and adequately protected, and to ensure that the Office of the Data Protection Commissioner is well-resourced (both administrative and financial), made operational and is empowered to operate independently . Given some of the areas of concerned outlined in our analysis, it is important that the Office of the Data Protection Commissioner address rapidly some of these issues by issuing recommendations and guidelines, outlining its interpretation of some provisions or aspects of a data protection law and clarifying the law as necessary.

---

[1] See Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 45 available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

[2] See the African Union Convention on Cyber security and Data Protection, 2014, available at http://pages.au.int/infosoc/cybersecurity

[3] See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonald ata.htm

[4] See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm

[5] See the Supplementary Act on personal data protection within ECOWAS, February 2010, at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf

Part I – Preliminary

Definitions (section 2)

The Act fails to clearly define some of the most fundamental and recurrent terms in the law. In particular we would like to outline the following comments with regards to the definitions provided for in the Bill.

'sensitive personal data'

There are a couple of omissions from this definition including membership of a trade union, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings. These should be included.

Object and purpose (section 3)

Echoing concerns, we flag further down in this submission Section 3 (b) fails to incorporate all of the internationally recognised data protection principles within this section of the Act even if they are provided for elsewhere in the law, including:

- Fairness and transparency
- Storage limitation
- Accountability

Part II – Establishment of the Office Of Data Protection Commissioner

Establishment of the Office and Appointment (section 5 & 6)

The establishment of the office of the data commissioner as a body corporate does not grant this office with the necessary institutional and financial independence to execute its mandate effectively under the new law. In order to ensure the necessary independence and effectiveness of the Office it should be Statutory Commission which would be preferred to a State Office.

Part III – Registration of Data Controllers and Data Processors

Application of Registration (section 19)

We welcome the additional details provided around the process for registration of data controllers and processors, but the following provisions require clarification to strengthen the right to information and the right to access provided for under section 26:

- Section 19 (2) (a): It is not sufficient to merely provide a "description" of the personal data to be processed. It should be clearly state what personal data will be processed.
- Section 19 (2) (b): It is not sufficient to merely provide a "description" of the purpose of processing. In accordance with the principle of purpose limitation, the purposes for which personal data are collected should be specified,
- Section 19(5): Whilst earlier versions of the law provided for an undefined "prescribed period", the Act does not impose any requirements on the timeframe to be respected by the data controller or data processor to notify the Data Commissioner of a change in any particular outlined under subsection (2). The law should not be silent on this requirement.

Compliance and audit (section 23)

The Act fails to outline what the criteria would be for the Data Commissioner to decide to carry out an audit of the systems of a data controller or data processor.

We would urge the Data Commissioner to develop and publish guidelines on the process for audits as soon as possible in order to clarify the decision-making process behind this section including who would be undertaking the audit. It is important that the audit be independent and effective.

Designation of the Data Protection Officer (section 24)

The use of the term 'may' in Section 24 (1) makes it unclear when the obligation to designate a data protection officer applies – it means that it appears optional as opposed to mandatory. The Data Commissioner should pronounce itself on this through subsequent regulations to delineate firms that will be required to employ/contract a data protection officer.

The law fails to define what constitutes "*regular and systematic monitoring of data subjects on a large scale"* as provided for in Section 24(1)(b). The Data Commissioner

should clarify this term in order to ensure that data controllers and data processors know when they are obliged to designate a DPO.

This section fails to outline details on the mandate and functions for the DPO, and so the Data Commissioner should develop guidance and guidelines on the role of a DPO and ensure it includes that they must be involved in a timely manner in issues related to data protection, that they have the necessary resources to carry out their tasks, that they are sufficiently independent and will not be dismissed or penalised for carrying out their tasks, and that they report to management (i.e. Board).

Part IV–Principles and Obligations of Personal Data Protection

This section of the Act is not well-structured and leads to confusion as it does clearly articulate each of the following: the data protection principles, the obligations on data processors and data controllers, and the rights of data subjects. Below we provide some suggestions on structure alongside the comments on this part as follows:"

Principles of data protection (section 25)

Section 25 is not complete and fails to outline all of the international recognised data protection principles. This section does not include principles provided elsewhere in the law, and this inconsistency is confusing.

- **Integrity and Confidentiality:** This principle is provided for in section 41 and 42 but it must also be listed here in section 25 for consistency.
- **Accountability:** Whilst this is provided for in Section 29, as it is a recognised principle the Act should also include a principle of accountability in this section too. An entity which processes personal data, in their capacity as data controllers or processors, should be accountable for complying with standards, and taking measure which give effect to the provisions provided for in a data protection law. Those with responsibility for data processing must be able to demonstrate *how* they comply with data protection legislation, including the principles, their obligations, and the rights of individuals.

Rights of a data subject (section 26)

A central component of any data protection law is the provision of the rights of *data subjects*. These rights should appear early in the law, as they should be seen as applying throughout, underpinning all provisions in the law. These rights impose

positive obligations on data controllers and should be enforceable before an independent data protection authority and courts.

Whilst there are provided elsewhere in the law, the following rights must also be listed under section 26:

- **The right to an effective remedy:** The law provides under Part VIII information on the ability for an individual to submit a complaint, but it is important that this be presented as a right under this section. It is a right of a data subject to access an effective remedy against a data controller and/or data processor, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law. Individuals should be empowered to take action themselves, as well as instructing others (including NGOs) to take action on their behalf.
- **Right to compensation and liability:** The law provides under Part VIII for compensation, but it is important to ensure it is listed here as a right. A person whose rights are found to have been violated should have a right to compensation for the damage suffered – material or non-material (e.g. distress).
- **The right to data portability:** Whilst the right to data portability is provided for in Section 38, it must also be listed in section 26.
- **The rights in relation to profiling and automated decision-making:** Whilst the right to not be subject to automated decision making is provided for in section 35 and includes right not to be subject to profiling, these should also be listed in section 26, ideally as separate rights.

Collection of personal data (section 28)

The principle behind section 28(1) is in the right place (despite the fact that this often doesn't happen in practice), however, it is undermined by the number of situations where it can be disapplied which are outlined in Section 28(2). In particular we are concerned with the following parts of this section:

- Section 28 (a): Just because data is a matter of public record does not mean that it is available for further processing, and its 'public' availability should not be construed as consent nor as another legal basis for further processing.
- Section 28 (b): Acknowledging the complexity of the data generation and processing ecosystem, a data subject "deliberately" making data public is not a sufficient justification for indirectly processing the data without involving the data subject.
- Section 28 (c): If consenting to collection from another source, they must be have been informed that there will be further processing and by who.

- Section 28 (e): The requirement that the collection "would not prejudice the interests of the data subject" is overly broad and could give rise to abuse.
- Section 28 (f) (iii): This provision is overly broad, in terms of what the protection of interests of another person are. It raises questions as to the intended purpose is: is it to be the vital interests of a natural person, or the commercial interests of a company or the political interests of a political party. The current wording is open to abuse.

The Data Commissioner should develop further regulation to address the above concerns in order to ensure that the right to information provided for under section 26 (a) is upheld effectively.

The requirements made by the Data Commissioner in relations to this section should be bolstered by requiring for a Data Protection Impact Assessment under section 31 to be undertaken to show that they understand the risks and effects of collecting, maintaining and disseminating personal data. It will also help to outline the appropriate policies to mitigate such risks. Such an assessment will also gauge whether the controller/processor complies with the legal and regulatory framework established under the bill.

Lawful processing of personal data (Section 30)

The Act fails to define what constitutes "public interest" in Section 30 (1) (iv) and (vi). The lack of definition, and clarity around what constitutes 'public interest' and its often-broad interpretation, raises concern that it can act as a loophole. A public interest ground should be clearly defined to avoid abuse. For example, it should be possible to list the specific public interest grounds and ensure that such a list is clear and exhaustive.

Section 30 (1)(vii) remains overly broad, in terms of what "the legitimate interests pursued by the data controller or data processor by a third party". It raises questions as to the intended purpose is of this provision. The current wording is open to abuse. If this provision is included and there is any doubt in the balancing exercise that there is prejudice to the individual, then the presumption should be that the processing should not go ahead. This provision should not apply to public authorities.

Data Protection Impact Assessment (Section 31)

We welcome the inclusion of this obligation for data controller and processor to undertake a data protection impact assessment. However, we believe the conditionality of the obligation as per Section 31 (1) to only comply when processing is

likely to result "in a high risk" to the rights and freedoms of data subject is too high. Whilst it particularly important to do them in such instance, we recommend that conducting an assessment should be an obligation prior to any processing activities.

Furthermore, this duty should be strengthened by specifying the means/form in which this right should be implemented. Consideration should be given to including requirements as to the form in which this information/ notice is provided to the data subject i.e. it should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Consideration must be given to ensure that those who are illiterate are not excluded from being informed, and alternative measures should be taken to communicate with them in a way that ensures they are adequately informed.

We urge the Data Commissioner to develop further guidance for data controllers and data processors on the threshold which triggers requirement to undertake a data protection impact assessment.

Conditions for consent (Section 32)

We welcome the addition of conditions for Consent. These are an important start in making consent meaningful in practice. However, it is still an issue which will require further consideration in terms of implementation and in particular guidance on the situations where consent is appropriate. We urge the Data Commissioner to articulate such guidance for data controllers and data processors.

Processing of personal data relating to a child (Section 33)

The section does not provide details on what constitutes a child for the purposes of this law, i.e. how old is a child? This section should be reconciled with the protection provided for in the Children Act which upholds the right to privacy under Article 19.

The sections to omit to clarify what constitutes "appropriate mechanisms for age verification" referred to in Section 33 (2) as well as "appropriate mechanisms for parental consent".

Safeguards should be provided against children's data being used for research or statistical purposes, and as noted elsewhere, the mere public availability of a child's data does not mean that it should be available for processing.

We urge the Data Commissioner to clearly address the aforementioned omitted information in this section in order to clarify the obligations related to the process of personal data relating to a child.

Automated individual decision making (section 35)

We welcome the inclusion of the right of a data subject not to be subject to automated decision making. However, the provisions fails distinguish between automated decision-making and profiling, and therefore the Act fails to provide for effective protections and rights in relation to both.

For profiling, it is important that individuals are aware when profiling will reveal sensitive personal data and that there are safeguards in place. Individuals' rights should also apply to the data that is inferred, predicted and derived as a result of profiling.

In addition to treating profiling separately from automated decision making, Section 35 falls shorts of imposing the necessary obligations on data controllers and data processors, and in particular in relations to the following shortcoming of the section:

- A data controllers and processors who profile to be transparent about it and individuals must be informed about its existence from the onset and not "as soon as reasonably practicable" as per Section 35 (3)(a).
- Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their rights, including to access, rectification and deletion.
- This right need to be applied to derived, inferred and predicted data, to the extent that they qualify as personal data.
- This Act should impose restrictions and safeguards on the ways in which data can be used to profile and make decisions.

The exemptions provided for in Section 35(2) must be limited, as well as clearly and narrowly defined. Even where exemptions allow for automated decision making, an individual should have the right to obtain human intervention, express their point of view and challenge the decision.

The Data Commissioner must take the lead to provide this clarity in further guidance on automated decision-making, and profiling.

Objecting to processing (Section 36)

This section alludes to the obligation of the data controller or data processor to demonstrate compelling legitimate grounds to overrule right to object of a data subject.

However, the section fails to ensure that the onus must be on the data controller or data processor to provide evidence for the need to continue processing the data of that individual, with reasons which override the interests, rights, and freedoms of that individual. Clarity must be provided on what "compelling legitimate grounds" are. The Data Commissioner must take the lead to provide this clarity in further guidance.

Limitation to retention of personal data (Section 39)

Exemptions for these purposes outlined in section 39 (1) should only be applied when strictly necessary and proportionate, and not been seen as a blanket exemption. The activities subject an exemption need to be clearly defined, for example, is research limited to academic research or does it include commercial research? There should be sufficient safeguards in place to protect the rights of data subjects.

Clarity must be provided for in terms of the applicability of the Data Protection Act in relations to other laws which imposed data retention policies such as the Kenya Information and Communications Act (2009) which regulates the retention of electronic records and of "information in original form", and the Kenya Information and Communications (Registration of Subscribers of Telecommunication Services) Regulations (2015).

Data protection standards should be applied as far as possible and detailed consideration should be given to any limitation on the rights of data subjects and the relevant data controllers should consider and mitigate any prejudice to the rights and freedoms of the data subjects. This is particular crucial when retaining data about key populations who may be exposed to risks should their data be unlawful processed and so measures should be taken to minimise the retention of their data, along with other security measures, to mitigate the possible risk of a breach. A data subject should be given the right to object that their data be processed for these purposes.
Furthermore, whilst rarely noted within this provision as an exemption, we would suggest that this exemption apply under certain conditions to research carried out by independent non-governmental, non-for-profit organisations.
In relation to section 39(2) it is important to note that pseudonymised data is still personal data and therefore still subject to the protections of the law and not processed in this form longer than necessary.

Right to rectification and erasure (Section 40)

This section lacks clarity as to the factors to be considered when deciding on a data subject's request to delete information.

It is important that provision is made to ensure among other safeguards, that when processing the request for deletion, the data controller considers the public interest of the data remaining available. It is essential that any such right clearly provides safeguards and in particular exemptions for freedom of expression and freedom of information. The construction of this right and how it will play out in the national context must be considered very carefully to ensure that it is not open to abuse.

Notification of breach of security on personal data (Section 43)

Breach notifications are essential to a data protection law and to ensure transparency on part of the data controller. However, the threshold to only notify when there is "real risk of harm to the data subject" is vague and no criteria of risk and likelihood is laid down in the section. The vagueness can constitute a loopholes for data controllers who hide behind subjective determinations of risk.

Clarity is needed on section 43(3) and what this justification for delaying notification means.

It is imperative that for a breach notification to be meaningful for data subjects, the notification should be in clear and plain language and includes advice and the tools to take measures to protect from harm and to seek redress from harm suffered. Consideration must be given to ensure that those who are illiterate are not excluded and that the data controller takes necessary measures to ensure they are informed.

We are concerned by the exemption provided for in Section 43(6) which provides that the obligation to notify does not apply if the data affected was encrypted. There is no guarantee that even if it was encrypted that the data won't be accessible to the person who unlawful obtained the data at that point in time or at a later stage should they acquire the means to decrypt the data.

Part V – Grounds for Processing of Sensitive Personal Data

Processing of personal sensitive data (Section 44)

In relations to section 44(1) consideration must be given the concerns presented in this submission with regards to the shortcomings of section 30 'Lawful processing of personal data'.

Permitted grounds for processing of personal sensitive data (Section 45)

It should be clear that one of these grounds must be satisfied in addition to a ground under section 30.

We reject the ground for processing sensitive personal data provided for in section 45(1)(b). Noting the complexity of the data generation and processing ecosystem, a data subject "manifestly" making data public is not a sufficient justification for indirectly processing the data without involving the data subject, particularly when it comes to sensitive personal data.

We challenge the ground for processing sensitive personal data provided for in section 45(1)(c)(ii) which refers to "rights of the controller". A data controller does not have rights, in the same way a data subject has rights and if it is legal obligations that are being referred to this should be clear.

In processing sensitive personal data, at minimum the following protections should be included:

- a prohibition on processing sensitive (or special category) personal data unless a specific narrow exemption applies;
- limits on the use of sensitive personal data for automated-decision-making;
- safeguards for international transfers; and record-keeping and data protection impact assessment obligations.

The sensitivity of the data should also be considered in enforcement and redress mechanisms. If these protections can be strengthened through sectoral regulation (for example in the financial of health sector) then this is to be encouraged.

Further categories of sensitive personal data (section 47)

The threshold of risk provided for in Section 47(2)(a) and (c) is too high and must be revised to ensure the best interests and protection of the data subjects.

Part VI – Transfer of Personal Data outside Kenya

Conditions for transfer out of Kenya (section 48)

Clarity should be provided as to what is meant by 'proof' and 'appropriate safeguards' in section 48(a) and how this oversight and authorisation will work in practice.

As noted above, clarity should be provided on what is considered a matter of 'public interest in section 48(c)(iii), otherwise this provision is left open for abuse.

The provision under Section 48 (c)(v) remains overly broad, in terms of what the protection of "vital interests" of another person are. It raises questions as to the intended purpose is: is it to be the vital interests of a natural person, or the commercial interests of a company or the political interests of a political party. The current wording is open to abuse.

Consideration should be given to the removal of section 48(c)(vi), 'compelling legitimate interest' is not a defined term and is open to abuse. The provision does not provide enough safeguards for individuals.

We urge the Data Commissioner to provide clear definitions of the terms used in this section.

Processing through a data server or data centre in Kenya (Section 50)

We are concerned by the obligation under section 50 regarding the storage of data on a server or in a data centre located in Kenya. This sort of measures, often referred to as data localisation, does not per se protect the safety of personal data. If other jurisdictions offer an adequate level of protection, there is no justification based on safety of personal data for preventing their transfer or imposing the storage of the personal data in a particular country. Further, we note that in other jurisdictions the imposition of data localisation has been introduced as a way to facilitate unlawful surveillance and limiting the capacity of individuals to protect the confidentiality of their communications.

Firstly, we are concerned by the discretion awarded to the Cabinet Secretary under section 50). Secondly, "strategic interests of the state or on protection of revenue" is too vague and must be clearly defined and limited. Thirdly, is unclear what "critical personal data" means/ This term is not defined elsewhere in the Act. Clarity needs to be provided on what this term means.

The prohibition of cross border processing of sensitive personal data will also be extremely complex in practice and limit access to services and systems for people in Kenya.

VII – Exemptions

General exemptions (section 51)

The exemptions provided for in section 51 (2) are too broad and must be revised – in particular terms such as "national security" and "public order "which are not defined. Blanket exemptions are never justifiable. In the limited cases where an exemption is justifiable, it should only apply in limited circumstance. It is essential to ensure that any exemptions are:

1) clearly defined and prescribed by law;
2) respect individual's fundamental rights and freedoms,
3) are necessary and proportionate measures in a democratic society, and
4) are only applicable, where failure to do so prejudice the legitimate aim pursued.

Research, history and statistics (section 53)

In order to avoid abuse and wide interpretation of this exemption, the Data Commissioner must provide guidance to undertake the following:

- clarity on what the research, history and statistical purposes are. Further detail should be included within the law and/or guidance be developed to define this further.
- Such a ground must not exempt a data controller or processor from all of their obligations, and they should provide for appropriate safeguards for the processing of personal data for these purposes.
- Safeguards could include ensuring that the data will not be used to take decisions about the individuals and that the processing is prohibited if it would cause harm.
- A data subject should still have rights over their data including the right to be informed and the right to object that their data be processed for these purposes.

Part VIII – Enforcement Provisions

Complaints to the Data Commissioner (section 56)

The law should have also included provisions for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations processing personal information, which would benefit all those affected. Provision should therefore be made in the process to allow individuals to be represented by qualified representatives and for certain qualified bodies, such as non-profit groups working in the field of data protection, to make complaints and seek remedies.

Administrative Fines (section 63)

We welcome that inclusion of fines if there is an infringement of a provision of this Act. However, we would advocate for a wider variety of sanctions beyond administrative sanctions in case of non-compliance or breach of the Act. The types of sanctions/ penalties to consider including are:

- Criminal offences (individual responsibility) for certain actions, for example knowingly or recklessly, without the consent of the data controller, obtaining or disclosing personal data.
- Direct liability for directors of companies.

We recommend the Data Commissioner to explore further types of sanctions to be administered.

Part X – Provisions on Delegated Powers

Regulations (section 71)

The delegated powers afforded to the Cabinet Secretary under this section remain too wide. In particular section 71(2)(l) which allows them to make regulations in any other matter as they see fit.

The Data Commissioner will play an important to ensure that regulations respect the principles and obligations provided for in this Act, and the process of developing such regulations should subject to effective Parliamentary scrutiny.



Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471