Draft Comments on the Data Protection Bill, 2018

Presented to the Privacy and Data Protection Taskforce, Ministry of Information, Communications and Technology

October 2018

About us

This submission is made by the National Coalition of Human Rights Defenders – Kenya (NCHRD-K), the Centre for Intellectual Property and Information Technology (CIPIT) and Privacy International (PI).

The Centre for Intellectual Property and Information Technology (CIPIT) an evidence-based research and training think tank based at Strathmore University Law School, Nairobi, Kenya. Our Mission is to study, create, and share knowledge on the development of intellectual property and information technology, especially as they contribute to African Law and Human Rights. We take pride in furthering non-partisan research that is independent and objective. CIPIT has in the past been instrumental in helping to highlight some of the limitations facing data protection in Kenya most recent of which includes a study on the privacy implications of adopting biometrics in the 2017 Kenyan elections. The report was discussed in one of the events of the 62nd session of the African Charter for Human and Peoples Rights to inform the inclusion of the right to privacy to that Banjul Charter. In partnership with other stakeholders, CIPIT has also organized local forums and workshops to identify and debate the pertinent issues on the current legislative proposals.

The National Coalition of Human Rights Defenders-Kenya (NCHRD-K) 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.

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.

To find out more about privacy and data protection in Kenya, please refer to 'The State of Privacy in Kenya' (last updated in February 2018).

Contacts

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.org

Dr. Isaac Rutenberg
Director, CIPIT
irutenberg@strathmore.edu

Dr. Robert Muthuri
Senior Research Fellow – IT, CIPIT
rmuthuri@strathmore.edu

Kamau Ngugi
Executive Director, NCHRD-K
dkngugi@hrdcoalition.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 25 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.

Development of a effective and comprehensive Data Protection law in Kenya is a priority. In particular given that a number of strategies are currently being deployed in Kenya to promote digital inclusion including: digital identities, micro-lending and alternative credit Scoring. While these efforts have positive intentions, a number of concerns ought to be addressed and a strong data protection framework would be a step in the right direction, for example:

a) Firms should deploy secure infrastructures to avoid data breaches, like those currently being seen with the Aadhaar system in India.
b) Biometrics are used excessively in certain circumstance where less intrusive options such as unique identifiers would be sufficient without the concomitant risk. This is particularly true in the health sector where biometrics could expose certain at-risk populations.
c) Alternative Credit Scoring by Micro-Lending institutions use a vast range of data points such as call detail records (CDR) and customer relationship management (CRM) details. These firms are often acting without clear opt-in mechanisms or sufficient information being provided to individuals.

However, the Data Protection Bill proposed by the Taskforce has a number of significant shortcomings. We recommend that to effectively protect privacy and to meet international

[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. 45available 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] 3See 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

standards in protecting personal data, that full consideration be given to the areas of concern and improvements outlined below under each Part of the Bill, and include:

- Reviewing some of the definition outlined in Part 1 and in particular clarify the definition of 'sensitive personal data'.
- Reviewing the material and territorial scope of the law, in particular with the aim of ensuring that the law applies to public entities including law enforcement and intelligence agencies.
- Guaranteeing that all data protection principles are included and revised clearly to provide for principles of fairness and transparency, storage limitation, integrity and confidentiality, and accountability.
- Guaranteeing that data subjects are provided with rights including the right to suppress or block (restrict), the right to data portability, as well as the protection and enjoyment of their rights in relation to profiling and automated decision making.
- Reviewing the current scope of the obligation to notify a data subject about the processing of their personal data.
- Providing clarity as to what the legal grounds for processing may be including by defining concepts such as 'public interest' and 'legitimate interest', and in particular review the legal grounds for processing 'sensitive personal data' to strengthen the protection of such data.
- Ensuring that any exemptions relating to the different data protection principles and the rights of data subjects must be provided for in the law in a form which is clear, precise and limited to specific necessary and proportionate exceptions rather than broad blanket exemptions, particularly for government authorities.
- Reviewing the grounds for processing including ensuring that data processing of data which is available to the public or deemed publicly available is not free for all to use without requiring further involvement of the data subject.
- Reviewing the clause on the storage of data in Kenya and recommending that focus should be on ensuring the data is protected with the highest safeguards rather than demanding data localisation which may not achieve the purpose of providing a higher level of protection as intended.
- Guaranteeing that a strong process is in place to regulate the transfer of personal data including developing a process for assessing adequacy of protection in the receiving country, and not only in terms of data protection but protection of human rights and rule of law.
- Ensuring that the protection of the data subject and their data as well as their right of privacy is balanced with freedom of expression under Article 33 of the Constitution for the media, artistic or literary work.
- Guaranteeing that the independent authority established by the law, the Office of the Data Protection Commissioner, has sufficient resources to undertake its mandate, and

also that data subjects are given access to an effective remedy and ensuring that the Commissioner has the power to impose penalties, and ensure effective remedies.

Part I – Preliminary

Definitions (clause 2)

The most fundamental and recurrent terms in the law must be clearly defined at the outset. 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. Furthermore, clarity should be provided that by 'belief; the law includes religious or philosophical beliefs or other beliefs of a similar nature.

'data subject'
The definition of a data subject needs clarification, to make it clear that the data subject is the person to whom the personal data relates.

Object and purpose (3)

Echoing concerns we flag further down in this submission Clause 3 (c) fails to incorporate all of the internationally recognised data protection principles within this section of the Bill, including:

- Fairness and transparency
- Storage limitation
- Accountability

Application (Clause 4)

We would like to seek clarification of the scope and application of Clause 4(b) (ii). What does it mean when it reads the Act applies to data controllers and processors who are not established in Kenya but "uses equipment in the Kenya for processing personal." It is unclear what this sentence means and also what the terms "uses" and "equipment" mean in this provision.

The scope of the Act as set out in clause 4(b) provides limited protection for the personal data of people in Kenya as (i) a controller or processor established in Kenya can easily remove its processing from the scope of the Act by conducting the processing outside Kenya and (ii) even where the law seeks to capture those controllers/ processers not established in Kenya it limits the scope to where the processing uses equipment in Kenya – thus removing from scope many data processing operations involving the data of people in Kenya.

We are concerned by the blanket exemption provided for in Clause 4 (2) (a) which notes that the Act would not apply *to "the exchange of information between government departments and public sector agencies where such exchange is required on a need-to-know basis."* Whilst some limited exemptions may be legitimate in these instances, these must be clearly defined in the law, necessary and proportionate and must be the exception not the rule.
We are concerned by the blanket exemption provided for in Clause 4 (2) (c) as per our comments on Part VII (*see below).*

PART II – OFFICE OF DATA PROTECTION COMMISSIONER

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

The legislative proposal opts for a body corporate to oversee implementation of the proposed regulatory framework. It is essential to guarantee the actual and perceived independence of the oversight institution/ regulator. The current provision of appointment by the Cabinet Secretary risks making the Commissioner too dependent on the appointing ministry which could mean that office holders would not enjoy the security of tenure necessary to carry out their duties with full confidence and independence.

Consideration should be given to establishing the Office of the Data Protection Commissioner as a Commission instead of body corporate. A Commission is an option that has been taken up in the African context for instance in Ghana. This will also help ensure the institution's perceived financial independence as an Article 254 Commission.

In the same vein and for the same reasons, the Public Service Commission, and not the Cabinet Secretary of the appointing ministry, could oversee appointment of the Commissioners to serve on the proposed Commission.

Powers of the Data Commissioner (clause 5)

Whilst we welcome the range of powers given to the Office of the Data Protection Commissioner we would suggest further details be provided on how it is ensured that the Commission has sufficient independence and resources to effectively undertake its mandate.

We also note that the failure of the Act to provide the Office with the power to impose appropriate penalties, including fines, enforcement notices, undertakings, and prosecution. This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority.

Removal of the Data Commissioner (Clause 11)

The Bill must clearly explain the process which would oversee the removal of the Data Commissioner, and in particular it must clearly note who would be responsible for initiating and/or overseeing this process.

PART III – REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Application of Registration (Clause 16)

It is not clear what "criteria" Clause 16(4) refers to in this instance, and it is unclear what is the "prescribed period" noted in Clause 16(5). It should be clear whether there are to be any exemptions to registration and if so the basis on which such a decision is to be taken. Consideration needs to be given to a variety of factors including size, volume, sensitivity of data as well as the sector of the data controller – for example, a start-up or SME might be handling a significant amount of sensitive data.

Compliance and audit (Clause 20)

It is unclear 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 like to request further clarity on the decision-making process behind this clause.

Designation of the Data Protection Officer (Clause 21)

The use of the term 'may' makes it unclear when the obligation to designate a data protection officer applies – it means that it appears optional as opposed to mandatory. What constitutes "*regular and systematic monitoring of data subjects on a large scale"* as noted in Clause 21(1)(b) and *"large scale*" in Clause 21(1)(c). Further clarity should be provided on these terms, so data controller and data processors know when they are obliged to designate a DPO.

This provision should be strengthened by including further details on the mandate and functions for the DPO including that they 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

Principles of data protection (clause 22)

Clause 22 should be strengthened by providing clear and coherent principles. In particular, this clause would be strengthened if it included the following principles:

- **Integrity and Confidentiality:** This principle is provided for in Clause 37 but it must also be listed here in clause 22 for consistency.

- **Accountability:** The Bill should also include a principle of accountability. 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 (clause 23)

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.

We welcome the inclusion of the current rights under clause 23. However, there are several rights missing for the current Bill including, which we would urge be included:

The right to suppress or block: Whilst this right is provided for in Clause 30, it must also be listed in Clause 23.

The right to data portability: Whilst the right to data portability is provided for in Clause 34, it must also be listed in Clause 23.
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 Clause 31 and includes right not to be subject to profiling, these should also be listed in Clause 23, ideally as separate rights.

Collection of personal data (clause 25)

The principle behind Clause 25(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 Clause 25(2). In particular we are concerned with the following parts of this clause:

- Clause 25 (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.
- Clause 25 (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.
- Clause 25 (c): If consenting to collection from another source, they must be have been informed that there will be further processing and by who.
- Clause 25 (e): The requirement that the collection "would not prejudice the interests of the data subject" is overly broad and could give rise to abuse.
- Clause 25 (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. Similarly, the term "in the interest of national security" under clause 25(f)(v) is too broad and must be clearly defined.

- Clause 25 (g): As it currently reads it seems to indicate that if compliance is not reasonably practical the law need not be complied with if it is too much effort. This is also open to abuse and wide interpretation and should be removed.

This clause should be bolstered by a clause that requires firms to conduct a Data Protection Impact Assessment 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.

Duty to notify (clause 26)

The right of individuals to know what personal data that controllers hold on them is a fundamental component to data protection law.

The UN Human Rights Committee, in interpreting the scope of obligations of states parties to the International Covenant on Civil and Political Rights, noted, back in 1989, that:
"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination." (Human Rights Committee, General Comment No 16 on Article 17 of ICCPR.)

More recently in its 2018 annual report on "The right to privacy in the digital age", the Office High Commissioner for Human Rights noted that "The individuals whose personal data are being processed should be informed about the data processing, its circumstances, character and scope, including through transparent data privacy policies." (A/HRC/39/29, para 29)

The qualification of "reasonably practicable" in clause 26 (1) is open to abuse. A specific time period should be provided.

The information to be provided in clause 26(1) should additionally include:

- the purposes of the processing;
- a description of the personal data;
- the legal basis for the processing
- the third-parties to whom the personal data has been or will be disclosed;

- the third-parties to whom the personal data has been or will be transferred, including details of safeguards adopted;
- the envisaged time limits for deletion of the different categories of data;
- a description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data.

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 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.

Lawful processing of personal data (clause 27)

Clarity should be provided as to how the various legal basis provided in clause 27 are compatible with the principle set out above that processing should be based on consent.

For clarity and to avoid abuse, 'natural' before person needs to be added to clause 27 (1)(iii).

We would like to seek clarity was to what constitutes "public interest" in Clause 27 (1) (iii) 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.

Clause 27 (1)(vii) is 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 public authorities.

In order to avoid any abuse and wide interpretation of Clause 27 (1)(viii), the following must be considered:

- There is a need for clarity on what the statistical and scientific 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.

The threshold in clause 27(3) on which it is decided that an impact assessment is required is too high. This threshold must be revised to not be to the detriment of the data subject.

The sanction provided for in Clause 27 (4) is not sufficient. First as noted above, it is unclear who would impose the fine given the failure of the law to clearly provide for the Officer of the Data Protection Commissioner to have the power to impose penalties/sanctions. Furthermore, a fine of KES 5,000,000 can be easily absorbed by most corporates leveraging data technologies in the country and should therefore be raised significantly in line with emerging practice worldwide.

Conditions for consent clause 28)

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.

Processing of personal data relating to a child (clause 29)

This clause must clarify what constitutes a child for the purposes of this law, i.e. how old is a child? This clause should be reconciled with the protection provided for in the Children Act which upholds the right to privacy under Article 19.

Clarity is sought as to what constitutes "appropriate mechanisms for age verification" referred to in clause29(2) as well as "appropriate mechanisms for parental consent".
We question the use of the term "guardian" in clause 29(3) and the role of the Commissioner is appointing them. This leads to unnecessary conclusion. Instead those data controllers or data processors falling within clause 29(3) a) or b) should be barred from the activities outlined in clause (4).

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.

Automated individual decision making (clause 31)

We welcome the inclusion of the right of a data subject not to be subject to automated decision making. However, it is important to distinguish between automated decision-making and profiling. The Bill should provide for effective protections and rights in relation to both. They do not need to be dealt with together (indeed this can lead to unnecessary confusion) but it is important that in relation to both there are requirements as to transparency, so that individuals are aware of the existence of these forms of processing.

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, Clause 31 should be strengthened by including the following obligations and key considerations:

- A data controllers and processors who profile to be transparent about it and individuals must be informed about its existence.
- 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 bill should impose restrictions and safeguards on the ways in which data can be used to profile and make decisions.

The exemptions provided for in Clause 31(2) must be limited, as well as and 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.

Objecting to processing (clause 32)

This clause 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, we would like to stress once again that 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.

Limitation to retention of personal data (clause 35)

Exemptions for these purposes outlined in clause 35 (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 clause 35(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 (clause 36)

This clause 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 (clause 38)

The law should be clear on a specific timescale for notification to data subjects. It is not clear what the 'prescribed period' in clause 38 is. In other jurisdictions, a specific timeframe is provided in number of hours after becoming aware of a breach, for example 72 hours.

Clarity is needed on clause 38(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 Clause 38(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 (clause 39)

In relations to clause 39(1) consideration must be given the concerns presented in this submission with regards to the shortcomings of clause 27 'Lawful processing of personal data'.

Permitted grounds for processing of personal sensitive data (clause 40)

It should be clear that one of these grounds must be satisfied in addition to a ground under clause 27.

We reject the ground for processing sensitive personal data provided for in clause 40(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 clause 40(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 (clause 43)

The threshold of risk provided for in Clause 43(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

Rules as to data centres and servers (clause 44)

We are concerned by the obligation under clause 44 (1) 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 clause 44(2). 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 bill. 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. The Bill should instead focus on building in safeguards.

Conditions for transfer out of Kenya (clause 45)

Clarity should be provided as to what is meant by 'proof' and 'appropriate safeguards' in clause 45(1)(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 clause 45(1)(iii), otherwise this provision is left open for abuse.

Consideration should be given to the removal of clause 45(1)(vi), 'compelling legitimate interest' is not a defined term and is open to abuse. The provision does not provide enough safeguards for individuals.

Safeguards prior to cross border transfer (clause 46)

The need to demonstrate adequate level of protection by the data controller or processors should not be limited to "security safeguards" as provided for in clause 46 but this obligation must apply to demonstrating an adequate level of protection in relation to all of the data protection principles as well as protection for human rights and the rule of law more generally.

VII – EXEMPTIONS

General exemptions (clause 47)

The exemptions provided for in clause 47 (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.

We are also concerned by the discretion awarded to the Cabinet Secretary to determine what constitutes an exemption by issuing a certificate under clause 47(3) thus bypassing effective parliamentary scrutiny. We recommend that the Bill is amended to limit such broad powers awarded to the Cabinet Secretary, and to ensure that any exemptions from the Act be subject to an open, inclusive and transparent legislative process. As a minimum any certificate process must be transparent both in terms of the procedure for issuing, the format of the certificates, and to whom they are awarded. Certificates must be limited both in time and in scope. There must also be oversight, with the certificates being independently reviewed (post issuing) as to their necessity and proportionality.

Research, history and statistics (clause 49)

In order to avoid abuse and wide interpretation of this exemption:

- There is a need for 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.

Exemptions by the Cabinet Secretary (clause 50)

We are also concerned by the wide discretion awarded to the Cabinet Secretary to determine what constitutes an exemption under this provision of the Act thus bypassing effective parliamentary scrutiny. We recommend that the Bill is amended to limit such broad powers awarded to the Cabinet Secretary, and to ensure that any exemptions from the Act be subject to an open, inclusive and transparent legislative process.

PART VIII – ENFORCEMENT PROVISIONS

Complaints to the Data Commissioner (clause 51)

We are concerned that clause (51)(b) fails to provide further details on what avenues would be open to a data subject should the Data Commissioner be "unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned".

As noted above under Clause 5, whilst we welcome the range of powers given to the Office of the Data Protection Commissioner we note that the failure of the Act to provide the Office with the power to impose appropriate civil penalties, including fines, enforcement notices and undertakings. This process of sanction should not depend on submission of the complaint by a data subject but can be imposed pro-actively by the independent data protection authority.

We would also to stress the right of data subjects in relations to having access to an effective remedy and the right to compensation:

- **The right to an effective remedy:** The law must include the right of an individual to 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. A data subject must have the right to submit a complaint to the independent supervisory authority. This reaffirms the need for the independent supervisory authority to have the power to receive complaints from data subjects, investigate them, and sanction the violator within their own scope of powers - or refer the case to a court. The law should also provide for the data subject to take action against a supervisory authority where they have failed to deal with their complaint. As well as the right to complain to a supervisory authority, individuals should also have access to an effective judicial remedy via the courts. 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:** 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). This underlines the need for robust enforcement models to be in place to ensure that any violation can be investigated and acted upon by a relevant authority, in this case the Office of the Data Protection Commissioner.

Furthermore, the law should also include 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.

Part X – OFFENCES AND MISCELLANEOUS PROVISIONS

General penalty (clause 59)

It is not clear what the role of the Data Commissioner will be in relation to an offence. Will they have the power to bring the prosecution or be consulted by the prosecution authorities or the Court? In terms of the amount there is also the question, particularly in the absence of civil penalties whether it would be more effective to include the option of a maximum penalty based on the % of the controller or processors annual worldwide turnover.

Regulations (clause 61)

The delegated powers afforded to the Cabinet Secretary under this clause are too wide. In particular clause 61(f) which allows them to make regulations in any other matter as they see fit. As much as possible the provision should be made on the face of the Bill and subject to effective Parliamentary scrutiny.