Submission of Comments on the Data Protection Bill, 2018

July 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), KELIN and Privacy International (PI).

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.

The Centre for Intellectual Property and Information Technology Law (CIPIT) is a think tank and training centre established under Strathmore Law School. 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. Our team is multidisciplinary, drawn from law, political science, computer science and development while using diverse methodological approaches to inform debates on ICT applications and regulation. The investigation into the legal and regulatory implications of technological advancement, including Big Data, as well as data privacy and security, is a key part of our mandate.

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.

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

Kamau Ngugi

Executive Director, NCHRD-K
dkngugi@hrdcoalition.org

Dr. Isaac Rutenberg
Director, Centre for Intellectual Property and Information Technology (CIPIT)
irutenberg@strathmore.edu

Allan Maleche
Executive Director, KELIN
Amaleche@kelinkenya.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 through the adoption of a Data Protection Act. We particular appreciate the direct reference to this Constitutional right under Clause 5, and the way it is referred to on several occasion in this proposed Bill.

However, the Data Protection Bill proposed by the Senate has a number of significant shortcomings. We recommend that to effectively protect privacy and to meet international 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 following:
  - the difference between agency and data controller,
  - that term data controller applies to both private and public entities,
  - that data subject is a natural person,
  - exempt information,
  - a broader definition of special personal information,
  - add a definition for consent as discussed in Part III clause 24 below; and
  - add definition of unique identifiers and biometric data.
- Reviewing the interchangeable use of certain words including 'controller' and 'agency, and 'information' and 'data', in order to prevent misinterpretation and provide further clarity of the protections and obligations provided for in the law.
- Reviewing the material and territorial scope of the law, in particular with the aim of clarifying 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, data minimisation and accountability.

[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/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.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

- 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 relations to profiling and automated decision making.
- Reviewing duty to notify with aim of providing further clarify on obligations of data controllers.
- Ensuring that all exemptions relating to the different data protection principles must be provided for in the law in a form which is clear, precise and limited to specific exceptions rather than broad blanket exemptions.
- Considering reviewing current proposal for the independent supervisory authority to ensure the Commission to be established is administratively and financially independent of any public authority and is given the necessary powers and adequate resources to conduct fulfil its mandate as an oversight and enforcing mechanism for this 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.

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.

'agency'
This term is somewhat confusing and appears to be used interchangeably with the term 'data controller', also defined in this section, throughout the Bill. We strongly suggest this be clarified to avoid any misunderstandings as to who has to comply with the law.

'data'
The definition of data under clause (3)(e) should include information recorded and held by both public and private entities

'Commission'
We have some reservations with the appointment of the Kenya National Commission on Human Rights as the independent authority mandated to oversee the implementation and enforcement of this law unless it is ensured that they have the administrative and financial independence they need as well as the necessary resources and powers to effectively undertake this new regulatory mandate. An alternative option for consideration is for the mandate of the Commission on Administrative Justice otherwise known as the Office of the Ombudsman, who is already handling the Access to Information regime, to be appointed to oversee and enforce the Data Protection Act. Our views on this are set out in more detail in relation Part IV below.

'data controller'
The Bill needs to clarify that it applies to both public and private entities. It should be explicit that public bodies, including law enforcement and intelligence agencies, are not excluded from the scope of the law.

'**data processer**'
There is no definition of a data processor. This definition is pivotal as it helps define and differentiate the different roles between the processor and the data controller. This particularly important to the principal – agent relationship and possible multiplicity between these two entities.

'data subject'
This definition is confusing as it refers to person, which as later defined includes a company, association or other body of persons whether incorporated or unincorporated (as per Article 260 of the Kenyan Constitution). The Bill should be clear that data subject is a natural person rather than a corporate entity. The second problematic element is that 'a data subject' is defined as the person from whom the personal data is 'obtained', however, the source of the data is often in practice not the individual to whom the data relates. Even if the language within the Bill provides some clarity, the definition of data subject should be revised to be clear from the onset that it is the natural person to whom the information relates.

'exempt information'
Applying the same broad exemptions as in the Access to Information Act does not consider that the scope of the Data Protection Bill is information relating to individuals to which they have a right.

'person'
We would like to seek clarification in relations to the reference to 'a person' as defined in Article 260 of the Kenyan Constitution. It is unclear what this term refers to in particular in relations to the definitions of 'data subject' and 'data controller' as noted above.

'personal data'
This definition does not address the question of identifiability, specifically indirect identifiability. It is essential that the definition recognise that personal data should include data that combined with other data relates to an identifiable individual. That said, before listing different categories of data, the definition should precede with a general definition that incorporates the different components for identifiability. The definition is not exhaustive, but it should also give explicit recognition to online identifiers, (this could be IP addresses, cookie IDs, advertising IDs); location data; genetic data; and a comprehensive definition of biometrics (fingerprints and blood types are unnecessarily narrow).

We would recommend that the Senate addresses this issue of indirectly identifiable data in the law and if necessary adopt measures requiring the independent competent authority to develop guidance and keep this issue under review.

'**special personal information'**
Sensitive or special data can be revealed from other data; therefore, the definition should specify that 'special personal information' means personal data that can reveal the specified categories. A glaring omission from this definition is data about an individual's sex, gender, marital status, sex life and/or sexual orientation. This should be included. Consideration should also be given to specific inclusion of genetic data.

Furthermore, some consideration should be given as to whether there are any other categories specific to the Kenyan context that should be added. Considering the local context and realities is an important step in ensuring that relevant safeguards are provided for in legislation.

It is also important that higher protections extend to data which *reveals* sensitive personal data, through profiling and the use of proxy information (for example, using someone's purchase history to infer a health condition), it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data.

Scope (clause 3)

The limited scope of the Bill give rise to concern. The exemptions for public bodies contained within clause 3 are overly broad. There is no justification for such broad, undefined and non-exhaustive (i.e. 'including') blanket exemptions.

Any exceptions should be in pursuit of a legitimate aim, limited, be clearly outlined, precise and unambiguous, narrowly interpreted according to principles of necessity and proportionality to ensure that the protections provided for within a data protection law are not made redundant. The exemptions to the Act should be deleted and must at the very least be further defined, restricted (they should not cover the whole Act) and be harm/ prejudiced based.

The Bill should also clarify that household activities by individuals are not included within the scope.

Part II – Objects and Principles of Protection of Personal Data

Principles (clause 4)

Clause 4 should be strengthened by providing clear and coherent principles. In particular, this clause would be strengthened if it included the following principles:

- **Fairness and transparency**: Personal data must be processed in a fair and transparent manner. This principle is key to addressing practices such as the selling and/or transfer of personal data that is fraudulently obtained. 'Fairness and transparency' are essential for ensuring that people's data is not used in ways they would not expect. This complements the principles of 'Lawfulness' provided for in clause (4) (a). With the principles currently provided for in (4) (b) and (c) are heavily reliant on consent, and this may be problematic in practice, it is particularly important to include the principles of 'fairness and transparency'.

- **Data minimisation:** We would recommend that the principles of 'data minimisation' be added to clause 4. Data minimisation is a key concept in data protection, both from an individual's rights and an information security perspective. The law should clearly stipulate that only the data which is necessary and relevant for the purpose stated should be processed. Any exceptions to this must be very limited and clearly defined. Requiring a test of 'necessity' ensures that the data collected is not intended to be more far-reaching than is necessary for the purposes for which the data will be used. The test should be that the least intrusive method is used to achieve a legitimate aim.

- **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.

Limitations (clause 6)

This clause gives rise to serious concern. It seeks to limit a constitutional right on the basis of 'safeguarding overriding legitimate interests'. Clause 6(2) goes even further and seeks to limit the right to privacy (not even just in terms of respect of personal data) on the basis of a number of broad purposes. At a minimum they require further definition and limitation including regarding harm, necessity and proportionality.

Any limitation to the right to privacy should respect the grounds for limitation of rights and fundamental freedoms provided for under Article 24 of the Constitution which upholds that: *"A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors"*.

This is particularly important in relations to processing by law enforcement and intelligence agencies. It is unacceptable practice that public institutions (including law enforcement and intelligence agencies) be completely exempt from having obligations to protect the personal data of data subjects, or for exemptions to be excessively wide or vague.

The data protection law should specifically provide for the development and inclusion of standards applicable to the protection of personal data which is collected and processed for the purposes of public safety, defence, state security and investigation or prevention of criminal offences. These provisions should, at a minimum, identify the public bodies mandated to collect and process personal data, fully respect and protect the right to privacy, and comply with the principles of legality, necessity and proportionality identified by international human rights experts, all under the supervision of an external body.

Collection of data from data subject (clause 7)

The principle behind this clause 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 this clause. In particular we are concerned with the following parts of this clause:

- Subsection 7 (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 a legal basis for processing.
- Subsection 7 (d): The requirement that the collection "would not prejudice the interests of the data subject" is overly broad and could give rise to abuse.
- Subsection 7 (e) (ii): 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.
- Subsection 7 (f): 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.

Furthermore, the aforementioned confusing definition and use of the term 'agency' renders this clause further concerning. There is a need to clarify that the obligations provided for in clause 7 apply to 'data controllers' and 'data processors'.

This clause should generally be subsumed 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 firm complies with the legal and regulatory framework established under the bill.

Rights of a data subject (clause 9)

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 independent data protection authority and courts.

We welcome the inclusion of the current rights under clause 9. However, there are several rights missing for the current Bill including, which we would urge the Senate to include:

The right to suppress or block: In particular circumstances, a data subject should have a right to suppress or block (restrict) the processing of their personal data, for example when the accuracy is in dispute so that the data is no longer used to take decisions about an individual. Personal data can then be stored but not further processed until the issue is resolved. Consideration should be given to include this right.

The right to data portability: This is a right that is increasingly included in data protection frameworks around the world. This give the right to data subjects to request that personal data about themselves that is processed by the data controller be made available to them in a universally machine-readable format, and to have it transmitted to another service with the specific consent of that individual. This can be particularly useful in the context of certain types of processing to allow individuals to receive their data and have it transferred in an interoperable format – enabling people to switch between services more easily. This right is a step towards ensuring that the data subject is placed in a central position and has a full power over his or her personal data.

The rights in relation to profiling and automated decision-making: A data protection law should provide effective protection and rights in relation to both profiling and automated decision-making. This should include all of the above rights and those already provided for in the Bill being applied in the context of profiling and automated decision making to address specific concerns related to these ways of processing personal data. These rights do not need to be dealt with together as this can lead to unnecessary confusion. However, it is important that both are covered in a data protection framework.

- **Profiling:** Profiling, just as any form of data processing also needs a legal basis. The law should require that organisations who profile are transparent about it and individuals must be informed about its existence. Individuals must also be informed of inferences about sensitive preferences and characteristics, including when derived from data which is not per se sensitive. 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. Individual's rights need to be applied to derived, inferred and predicted data, to the extent that they qualify as personal data.

- **Automated decision making:** This bill should impose restrictions and safeguards on the ways in which data can be used to make decisions. Individuals should have a right not be subject to purely automated decision-making. The law may provide for certain exemptions, i.e. as when it is based on a law (e.g. fraud prevention), or when the individual has given their explicit consent. However, any such exemptions 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.

This right is particularly important in the context of Kenya, where with the success of Mpesa and other technologies, Kenya is quickly becoming the test bed for mobile technologies in fintech, health-tech, agri-tech and other such related applications. There is rising concern of the liberties taken by some firms with regard to the data they collect for their algorithms e.g. for alternative credit scoring in fintech. The users of these apps are those in vulnerable positions in Kenyan society and they may not have the autonomy to determine how their data is being monetised. Therefore, applications should clearly state how the algorithm works, the data points and thereby the personal data that they intend to collect and use in their algorithms. The data subject should be granted a mechanism to opt-out of any data point they feel ought not be used to profile them and/or make decisions about them.

Duty to inform (right to information (clause 10)

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.)

The qualification of "reasonably practicable" in clause 10 (1) is open to abuse. A specific time period should be provided.
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.
- The information provided should include the legal basis on which the data is to be processed and period of time for which it will be stored.
- Data subjects should be informed of all their rights as well as their rights to complain (and how) to the oversight body (in this case as it currently stands in the Bill it would be the Kenya National Commission of Human Rights) and to seek judicial remedy.

The qualification of "practicability" provided for in clause 10(3) is open to abuse and should be restricted.

When agency may not notify (clause 11)

This Clause 11(3) must be reviewed. As it is currently worded, it seems to imply that individuals are being asked to waive their rights.

Exemptions (clause 12)

The exemptions provided for in Clause 12 are overly broad, in particular, the following subsections are of concern, and must be reviewed:

- Subsection (a): Just because data is a matter of public record does not mean that it can be lawfully processed without having to comply with the obligations provided for in the Bill.
- Subsection (b): Further processing by a data controller of data collected by a third party should be subject to the same obligations provided for in the Bill.
- Subsection (c): The requirement that the collection "would not prejudice the interests of the data subject" is overly broad and could give rise to abuse.
- Subsection (d) (i): the non-exhaustive nature of this exemption for public entities is overly broad.
- Subsection (f): As it currently reads it seems to permit that if compliance is not reasonably practical the law need not be complied with if it's too much effort. This is also open to abuse and wide interpretation.

Prohibition of profiling (clause 13)

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.

We welcome the prohibition to subject a data subject to automated decision making. We would encourage that it should be clear that human intervention must be meaningful. This obligation positively reaffirms what we noted above, that individuals should have a right not be subject to purely automated decision-making, and even where exemptions allow for automated-decision making, an individual should have the right to obtain human intervention.

'A threat to maintenance of law' in clause 13(2) is open to abuse. We propose that in such circumstances the decision be subject to judicial oversight.

Notification of security compromises (clause 16)

The law should be clear on a specific timescale for notification to data subjects. In other jurisdictions, a specific timeframe is provided in number of hours after becoming aware of a breach, for example 72 hours.

In clause 16 (a), the current wording of *"as soon as reasonably practicable*" is overly vague and may lead to delays in notification, which in turn leaves individuals vulnerable and the regulator unaware.

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.

Access to personal data (clause 17)

As well as having access to the data an individual should be provided with a copy of it. Consideration should also be given as to the format in which the information should be provided to an individual in order that it is intelligible to them, with particular measures taken when the data subject is illiterate or faces other challenges to understand the information they are provided.

Under the Access to Information Act the general timescale is 21 days and there is a regime of prescribed fees. Given these requests relate to personal data, there should be an amendment to ensure that this access is free of charge.

If the procedure is not to be specified on the face of the legislation it is even more essential that clear guidance is provided (in particular for those entities not subject to/ familiar with the Access to Information regime).

Furthermore, as we noted above in our comments on "Rights of data subjects", we would encourage the Senate to consider including a right of data portability in a data protection law in order to ensure

that the data subject is placed in a central position and has a full power over his or her personal data. This would permit individuals to request that their data be made available to them in a universally machine-readable format or ported to another service with the specific consent of that individual.

Finally, in relation to clause 17(2), our comments on the definition of 'exempt information' noted above apply.

Correction and deletion of information (clause 18)

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. 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.

Retention of information (clause 19)

Exemptions for these purposes outlined in clause 19 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 (2014).

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.

Interference with personal data (clause 23)

Further consideration should be given to the wording of the offence and what is meant with 'interfere' or 'infringe'.

Clarity must also be provided as to whom this clause applies, as the use of the term 'person' as defined in the Bill seems to refer to a private individual versus a public or private entity.

Part III – Processing of Special Information

Processing of special information (clause 24)

Consent is not defined in the Bill, this is problematic throughout but specifically in relation to special information.

The Bill needs to defined consent as *"freely given", "specific", "informed"* and "*unambiguous*", and elaborate on definition and conditions of '*consent'* in Clause 24 (2) (a) in relation to the collection and processing of special personal data.

Express consent is also referred to (clause 21) but no definition is provided. Consent should be specific, informed and unambiguous. A definition of both forms of consent referred to in the Bill should be provided and if there is to be a higher level of express consent this must also apply to special information.

There should be safeguards on the use of special information for statistical and research purposes, for example that the data will not be used to make decisions about individuals.
Just because special information is publicly available it should not give free reign as to its processing.
The same comments made for clause 19 on statistical or research purposes apply to this provision.

As a 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 exemptions for processing sensitive personal data need to be clearly defined and narrowly construed. Consent, for example, should be explicit (rather than implied). 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.

Data subject's race or ethnic origin (clause 26)

The Bill fails to provide a lawful, necessary and proportionate justification as to why race or ethnic origin would be essential to the identification of a data subject. The Bill needs to further clarify this provision, or remove it if no lawful, necessary and proportionate justification is provided for instances where this data would be collected and processed.

If this clause is kept in the Bill then clear and specific safeguards should be provided for clause 26(a) and (b) in relations to the collection and processing of data on race or ethnic origin as these constitute 'special personal data' and must be subject to even higher safeguards and protections.

Personal data of children (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.
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.

Part IV – Oversight and Enforcement

Discretion not to take a complaint (clause 35)

The Bill must clarify what is meant by clause 35(d) which reads: *"the complainant does not have a personal interest in the subject matter of the complaint".*

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 V Miscellaneous Provisions

Appointment of the Commission

We welcome the decision of the Senate to include the establishment of an independent supervisory authority in the form of a Commission to oversee the implementation of the Act, and to be responsible for its enforcement.

We have some reservations with the decision for the Kenya National Commission on Human Rights (KNCHR) to take on the role of being the regulator.

The KNCHR was established as an independent body tasked by law to act as a watch-dog over the Government in the area of human rights, and provide key leadership in moving the country towards a human rights state, and whilst it has the power to investigate human right violations, under its current mandate and structure, the KNCHR has limited powers and resources to decide and enforce sanctions, administrative, civil and criminal, which should be provided for under the Bill and is currently missing.

Alternative option for consideration is for the mandate of the Commission on Administrative Justice otherwise known as the Office of the Ombudsman, who is already handling the Access to Information regime, to be appointed at the independent supervisory authority of this Act. However, this combination of functions should not contradict the mandate, functions and powers of the enforcement authority, or independence from the Executive.

If it is however decided that the KNCHR be appointed as the independent supervisory authority under this Act, the KNCHR's mandate, powers and functions will have to be reviewed and amended to empower it to have the necessary powers and resources to fulfil its mandate as the oversight body and enforcer of this Act. Certain procedures and protocols must be implemented to address any conflict of interest which may arise with its new role so as to ensure that its original mandate as a national human rights institution is not adversely impacted.

Projection against certain actions (clause 37)

The Bill needs to clarify what is meant by *"in good faith"* in clause 37 (1).

Offences (clause 38)

It is important that those private and public entities processing personal data are held responsible for failures to comply with the law and be subject to sanctions should they violate it. However, it is not clear from the Bill what administrative and civil consequences there are. The criminal offence penalties are extremely severe and the way they are outlined such as in clause 23 the offence lacks clarity.

The bill does not give the "Commission" powers to issue fines, which in other jurisdictions has served as a strong deterrent in the corporate sector. This must be reviewed in the Bill and given careful consideration when deciding who will be appointed in the role of "Commission" to oversee the implementation and enforcement of the law.

In a similar vein, a fine of KES 500,000 and 100,000/= as provided for in clause 38 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.