October, 2018

Mr. Jerome Ochieng
Principal Secretary, ICT & Innovation
Ministry of Information, Technology and Communication
pdp@information.go.ke; pdp@ca.go.ke

Submission of Comments on the Kenya Privacy and Data Protection Bill, 2018

We thank the Cabinet Secretary Ministry of Information and Communications Technology and the Task Force on Development of the Policy and Regulatory Framework for Privacy and Data Protection for the opportunity to provide comments on the bill. We commend the Task Force and the Ministry for ensuring strong protections for user privacy in this bill and believe that Kenya's law can be a model for other African nations.

We have focused our comments on the areas where we feel protections are missing and where your proposals and recommendations can be strengthened based on our experience and expertise advocating for individual security and privacy all over the world.

We appreciate the bill's aspiration to elaborate Article 31(c) and (d) of the Constitution of Kenya, 2010. We note that the *Data Protection Bill* sets out principles of data protection that are consistent with international standards and commend the approach to place users' rights at the center of the digital economy.

Mozilla is a global community of technologists, thinkers, and builders working together to keep the internet open, accessible, and secure. We are the creators of Firefox, an open source browser that hundreds of millions of people around the world use as their window to the web, as well as other products including Pocket, Rocket, and Focus. To fulfill the mission of keeping the web open and accessible to all, we are constantly investing in the security of our products and the privacy of our users.

Our commitment to user security and privacy can be seen both in the open source code of our products as well as in our policies. Consider, for example, Mozilla's Data Privacy Principles[1] which guide the development of our products and services:

1. No surprises
Use and share information in a way that is transparent and benefits the user.

2. User Control
Develop products and advocate for best practices that put users in control of their data and online experiences.

3. Limited data
Collect what we need, de-identify where we can and delete when no longer necessary.

4. Sensible settings
Design for a thoughtful balance of safety and user experience.

[1] https://www.mozilla.org/en-US/privacy/principles/

5. Defense in depth
Maintain multi-layered security controls and practices, many of which are publicly verifiable.

While we take action to protect our users' privacy and security every day, relying on these principles and other policies for guidance, we also believe in the importance of data protection law to ensure data controllers and processors are protecting the rights and interests of internet users. As we will elaborate on in this submission, we believe a strong data protection law requires:

1. The enshrinement of a robust framework of rights of individuals with meaningful user consent at its core;
2. Strong obligations on data controllers reflecting the significant responsibilities associated with collecting, storing, using, analyzing, and processing user data; and
3. Effective enforcement mechanisms including an empowered, independent, and well-resourced Data Protection Authority (DPA).

We look forward to continuing to engage with you and other stakeholders in the Kenyan government as work progresses to craft Kenya's historic first data protection law.

If you have any questions about our submission or if we can provide any additional information that would be helpful, please do not hesitate to contact Mozilla Policy Advisor Alice Munyua (amunyua@mozilla.com).

Executive Summary

Kenya is among the continent's most connected countries as well as a regional hub for digital start-ups and entrepreneurship.[2] Mobile network coverage penetration rate is at 88.7%, with more than 40 million mobile subscriptions. Over 99% of internet subscribers access the internet via mobile phones. Kenya has also seen significant growth in online government services, and processing of personal data by the government is needed in order to access most of these services. Indeed, the Government of Kenya is likely the largest data controller in the country. Kenya has a significant data economy spanning both public and private sector. All of these public and private services have accelerated the collection and analysis of personal data.

While some of this collection and processing is a function of an advancing digital economy, the lack of comprehensive personal data protection legislation exposes Kenyan citizens to risks of misuse of their personal data.

We commend the government for setting out a clear framework based on international good practice, and our comments are intended to support and improve this strong draft.

Independence and powers of the Data Protection Commissioner

To ensure effective enforcement mechanisms of the new Privacy and Data Protection legislation, we strongly support the bill's intention to have an independent Data Protection Commissioner (DPC). Unfortunately, several sections of the bill undermine this provision by subjugating the DPC to the Cabinet Secretary, Ministry of Information and Communication Technology. We recommend that authority to set the qualifications of and nominate the DPC

[2] https://ca.go.ke/document/annual-report-for-the-financial-year-2016-2017/

should rest with parliament and appointment should be made by the President. We propose additional powers and responsibilities be assigned to the DPC, which include issuing regulatory guidance, codes of practice to data controllers and processors, investigatory, adjudicatory, levying penalties and punitive measures, as well as providing redress and compensation to users when their rights have been violated. The DPC should also be empowered to promote public awareness and engage in capacity development activities.

Missing protections on users rights and data controller/processor obligations

We applaud the comprehensive provisions of rights of access, correction, right to seek confirmation, update, rectify, and object to processing, as well as data portability. We further welcome the restrictions imposed on data controllers and processors around purpose limitation, collection limitation, and data retention limitation.

We however, note that while the policy framework includes the principle of data minimization, the bill does not contain this obligation. We believe this obligation should be added to the legislation and that language should be added to clarify that where information is longer necessary for the purposes for which it was collected, it should be deleted.

We appreciate the importance placed on obtaining user consent in this bill. However, consent must be meaningful. We refer to guidance issued by Article 29 Working Party of the European Union Data Protection Authorities on the elements of valid consent, which must be free, informed, unambiguous, clear, specific, and capable of being withdrawn. This sets a high bar for data controllers and processors seeking to process personal data on the basis of consent. "Explicit consent" must be a requirement for processing of sensitive data. We recommend that the DPC issues guidelines on how requirements around consent in this bill should be interpreted.

Principles and Obligations of Personal Data Protection

We support strong obligations placed on data controllers and processors reflecting the significant responsibilities associated with collecting, storing, using, analyzing, and processing user data. We also propose stiffer penalties that will provide better incentives to data controllers and processors to abide by the provisions of this law. Strong penalties and a strong, independent regulator are critical to the effectiveness of data protection law.

All public and private sector data controllers and processors must be bound by a general duty to process data in a manner that respects the privacy of an individual and that provides security against data breaches.

Data protection officers

We note that the bill requires all controllers and processors to register with the DPC and designate a data protection officer. This obligation would place an undue burden on small and medium enterprises (SMEs) and startups, which play an important role in the Kenya's digital transformation. While we recommend greater regulatory oversight for data controllers and processors who process large volumes of data, particularly sensitive data, or otherwise pose an elevated risk to the privacy rights of users, we do not believe mandatory registration of all data controllers and processors is wise or worthwhile.

Security safeguards

Data controllers and processors should take appropriate and reasonable measures to safeguard the data that they have been entrusted with. The bill appears to obligate controllers and processors to use pseudonymization as a security tool. We respectfully caution against over reliance on only this technique as a safeguard as it may not be feasible in many use cases. We would instead recommend that all data controllers and processors be obligated to take appropriate and reasonable measures to safeguard the data that they have been entrusted with, whether via encryption, pseudonymization, or other means. Additionally, we recommend an obligation that all data controllers and processors encrypt sensitive personal data.

Data breaches

The bill proposes attribution of breaches that lead to the unauthorized disclosure of personal data, however, this is often very difficult and time consuming, even for the most well-resourced data controllers and processors. Furthermore, notification of an unauthorized disclosure to affected data subjects should not wait for attribution. We propose clarifying this provision to require attribution information to be included "where available." This will go a long way to ensuring that notification occurs in a timely manner and will provide greater legal clarity to data controllers and processors.

Protecting Children Personal Data

We are pleased to note that the bill contains provision protecting the right to privacy of children as provided under article 19 of the Children Act. We would encourage the Government of Kenya to reconcile this bill with the Children Act, 2001 to ensure legal clarity on the data protection rights of children and the obligations on data controllers and processors who process the personal data of children. We recommend clarifying the language of this section to specify that data controllers and processors should not *knowingly* market, track, or profile children *without the consent of their parental guardian*.

The "parental consent" requirement in the bill raises practical questions regarding its implementation. We propose further reflection on parental permission and recommend that the DPC be mandated to provide guidelines on the impact of data protection law on children and explore these proposed approaches, particularly those relating to age verification mechanisms.

We recommend deletion of the provision that mandates the DPC to appoint data controllers and processors as guardians. This provision creates substantial legal confusion and places additional primary and secondary liability on data controllers and processors who will be designated as guardians.

Protecting Personal Sensitive Data

We note with concern the discrepancy between the definition of sensitive personal data in the policy and in the text of the bill. While we believe the policy, language includes a progressive list of what should be considered sensitive personal data, there are several critical omissions. The list contained in the policy should replace the definition of sensitive personal data in the bill and should be further amended to include: official or national IDs, passwords, financial data, and location information. We also recommend that the DPC is empowered to assess and add to the definition and categories of sensitive data in an open consultation process.

Exemptions

We are concerned that some of the exemptions provided in the Bill do not appear to satisfy Article 24 of the Constitution, which provides for the right to privacy. While, we recognize that there may be legitimate reasons for various parts of the government to share information with each other on a "*need to know basis,*" this provision is quite broadly worded. Furthermore, while the obligation to seek consent may not apply in these scenarios, public authorities should still always be bound by the other principles of data protection including purpose limitation, collection limitation, security safeguards, etc.

In addition, exemptions for the purposes of investigating crimes, or for any other purposes related to maintaining public safety and national security must be understood as exemptions from seeking user consent, not from all data protection requirements. Law Enforcement Agencies must also be bound by requirements around data security, purpose limitation, collection limitation, the right to rectify, the right to erasure, etc. Data processing for public safety, national security and law enforcement must be "necessary and proportionate", and authorized by law.

The provision to exempt for the purposes of history, research, and statistics could be subject to abuse by data controllers and processors. We recommend clear definitions and limiting scope for research purposes that is aimed at or culminate in commercial exploitation.

Data localization

We note with concern provisions contained in the bill obligating data controllers to "ensure the storage, on a server or data center located in Kenya of at least one serving copy of personal data" and other prohibitions on the transfer of sensitive data outside Kenya.

Requiring data to be localized not only creates a security risk, with a central point of attack or single point of failure, but undermines efficiency and integrity of internet traffic. The requirement to store data or a copy of data locally, introduces potentially higher costs and actual limitations on technology innovation, development, and use, and introduces a conflict of laws situation for multinational companies.

We acknowledge that certain categories of personal data may need to be mandatorily stored within the country, with restricted data flows, due to the strategic and security interests at play. However, the bill leaves the definition of critical personal data entirely open to Government discretion and does not elucidate what such categories might be, nor any parameters to circumscribe this discretion. Since mandating data storage in Kenya generally amplifies the concerns of routing inefficiencies, increased costs, and security risks, this wide discretion is concerning.We recommend that categories of critical personal data that are currently localized in Kenya for strategic or security reasons be clearly stated. The open-ended mandate to the government to notify further categories should be removed.

In addition, we recognize the needs and compelling interests of both private and public data controllers and processors to process sensitive personal data outside of Kenya. For example, financial institutions (whether banks or public authorities) transfer financial information to check for fraud and terrorist financing, for example. This provision as currently written could be read to preclude Kenya's participation in the SWIFT network, which would be gravely detrimental to Kenya's financial sector and economic standing in the world.

We respectfully recommend that the if Government of Kenya is concerned about law enforcement access to data, a legal framework for surveillance with appropriate protections for users is developed, providing a lawful basis for the government to access data necessary for legal proceedings.

Reconciling the Data Protection Act with other laws

Kenya has statutes dating as far back as pre-independence. Some of these statues contain provisions that override this proposed bill, thereby threatening the good intentions of this framework. Such laws include: Preservation of Public Security Act, Official Secrets Act Cap 187, National Intelligence Service Act, 2012 and The Prevention of Terrorism Act No 30 of 2012 just to name a few. These laws have provisions authorizing the government to collect, process, and share data without consent in circumstances that are not well defined and therefore subject to misuse.

In order to give full effect to the strong protections contained in this legislation, we respectfully recommend a package of amendments be offered to revise the provisions in previous legislation.

Comments on specific provisions of the Kenya Privacy and Data Protection Bill 2018

Part II: An Empowered and Independent Data Protection Commissioner

We strongly support the bill's intention to have a Data Protection Commissioner, which is independent from the government. As Section 7(2) notes: *"In the exercise of his functions under this Act, the Data Commissioner shall act independently and shall not be subject to the direction or control of any other person or authority."*

Unfortunately, several provisions of the bill undermine this independence by making the Data Protection Commissioner answerable to the Cabinet Secretary, Ministry of Information and Communication Technology rather than the Parliament and the President.

We propose the following amendments:

Section 6 (1) *"The Data Commissioner shall be appointed by the Cabinet Secretary on a competitive basis and on such terms and conditions as may be specified in the instrument of appointment."*

This section anchors the commissioner's office, including the appointment, financing, reporting, and removal, to the Cabinet Secretary Ministry of Information and Communications Technology. Recognizing that data protection is a cross cutting issue and acknowledging the need for an independent DPC, we propose that the Public Service Commission (PSC) conduct the necessary nominations, which should be approved by the Parliament. The Data Commissioner should then be appointed by the President to ensure the independence of the data protection commission especially when overseeing public data controllers and processors. For comparison, the governors of the Central Bank of Kenya are similarly approved by the Parliament and appointed by the President.

Section 8 (1) *"The Data Commissioner shall have all the powers necessary for the performance of the functions under this Act."*

While we believe that Section 8(2) provides a good foundation of powers for the Office of the Data Protection Commissioner, we believe this legislation would gain greater clarity and strength by including a few additional powers. Specifically:

- Issuing regulatory guidance to data controllers and processors;
- Overseeing the development of and recognizing codes of practice;
- Levying penalties and other punitive measures on data controllers or processors who violate the provisions of this Act;
- Overseeing and where necessary requiring the provision of redress and remedy when a data subject's rights under this Act are violated;
- Promoting public awareness and understanding of the risks, rules, safeguards, obligations, and rights in respect of protection of personal data under this Act;
- Conducting multi stakeholder consultations and inquiries to better understand the field of data protection and the enforcement of this Act; and
- Implementing capacity building initiatives such as training with relevant stakeholders.

Throughout the bill, it is contemplated that the Office of the Data Protection Commissioner may prescribe certain procedures and promulgate new roles. We would recommend that when developing rules, regulations, guidelines, and procedures, the Data Protection Commissioner should conduct public consultations on the same prior to their entry into force.

Section 51 (1) *"The annual estimates shall be submitted to the Cabinet Secretary for tabling in parliament"*

To ensure the independence of the commission, the annual estimates should be submitted to Parliament by the Data Commissioner. In addition, the Commissioner should make reports and estimates public to ensure transparency and accountability.

Section 9. (1) *"The Data Commissioner may, subject to such conditions as the Data Commissioner may impose, delegate any power conferred under this Act or any other written law to-"*
Section 9 (1)(c) *"a recognized self-regulatory organization."*

Self-regulation is an ambiguous term and a reliance on self-regulation may erode the strength of the protections articulated in this bill. If this provision is included, we would recommend detailing with specificity which powers the Data Protection Commissioner can and cannot delegate. We would also recommend further articulating what types of entities qualify as a "self-regulatory organization." The powers of self-regulatory organizations should furthermore be narrowly tailored to avoid collusion. However, as noted in our comments on Section 8, we believe the Data Protection Commissioner should have the power to recognize codes of practice developed by data controllers and data processors.

Section 10 *"The Office of the Data Commissioner shall be vacant if the data commissioner-"*
Section 10(b) *"by notice in writing addressed to the Cabinet Secretary resigns from office"*

As mentioned above, the Data Commissioner should report to the Parliament and the President, not the Cabinet Secretary. Therefore, the resignation should be sent to the Parliament and the President.

Section 10(c)*"is convicted of an offence and sentenced to imprisonment for a term exceeding six months without the option of a fine"*

We propose deleting the clause of *"for a term exceeding six months without options of a fine"*. A commissioner convicted of any crime subject to imprisonment should not hold office.

Section 47(3) *"For purpose of subsection (2) (a) a certificate signed by the Cabinet Secretary shall be sufficient evidence of exemption from outlined provisions of this Act"*

This interferes with the independence of the Commissioner and creates an opportunity for abuse of power. More precision should be provided and less discretion.

Section 50 "Exemptions by the Cabinet Secretary" *"The Cabinet Secretary (CS) may prescribe other instances where compliance with certain provisions of this Act may be exempted"*
All the exemptions must be stipulated in the Act. We suggest that the Cabinet Secretary should be limited to making regulations to expand on these exceptions.

Part III: Registration of Data Controllers and Data Processors

Section 16 (1) *"Every person who intends to act as a data controller or data processor shall apply to the Data Commissioner in prescribed form"*.

Section 21 *"Designation of the Data Protection Officer"*

Section 21 (1) *"A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine"*

Requiring all data controllers and processors to register with the Data Commissioner and designate a data protection officer in particular, places an undue burden on small and medium enterprises (SMEs) and startups, which play an important role in the nation's digital transformation. We recommend an approach based on quantities of data handled and sensitivity, by providing for different levels in the registration of data processors and controllers. Specifically, we believe that only entities subject to this legislation that process a large volume of personal data, handle significant amounts of sensitive data, or otherwise have a heightened risk of harm from the processing they carry out should be required to have a DPO. Furthermore, we believe the regulatory model should be such that the Data Protection Commissioner notifies data controllers or processors when they meet this threshold (including information on how to appeal such a classification) rather than requiring all data controllers and processors to proactively register.

Section 21 (1) (1) A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where—

> *(a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;*

This exemption for the courts acting in their judicial capacity is unclear and unwise. Courts in Kenya frequently act as processors. As such, courts should also be required to designate a data protection officer.

Part IV: Principles and Obligations of Personal Data Protection

Consistent with the foundations of data protection, we are pleased to see that the bill contains a number of protections, in particular the rights to access, seek confirmation and rectify personal data, to object to processing, and data portability. We further welcome the restrictions imposed on data controllers and processors around inter alia purpose limitation, collection limitation, and data retention limitation. We are however concerned that while the policy framework includes the principle of data minimization, the bill does not obligate data controllers and processors to ensure personal data is relevant and limited to the purpose for which the data was collected. We propose inclusion of data minimization as an additional obligation.

We appreciate the importance placed on obtaining user consent in this bill. Indeed, consent is one important part of the data protection chain which includes, but is not limited to, additional links like privacy by design, storing and transmitting data securely, collection and purpose limitation, oversight by the data protection authority, data breach notification, etc. Of course, if the link of consent is weak or broken, the integrity of the rest of the chain is compromised.

Consent must also be meaningful. The example of the EU's "cookie banners" is illustrative. As part of the 2002/58/EC Electronic Privacy Directive update in 2009 in the EU, all websites in Europe have had to implement a notice to users that their site uses cookies. While implementation varies significantly from Member State to Member State, these notices regrettably do not deliver the promise of control, transparency, and choice as per the spirit and intent of the e-Privacy framework. Rather, the user "consents" by clicking on the banner, or in some implementations, consent is interpreted by scrolling down the page, but they do not have a meaningful choice in the case they object to the data collection processes, nor do they have real information about how many parties can access their data and for what purposes. Users must be given a real choice, and should not be forced into a "take it or leave it" approach where their only option is to accept a given service or site's terms of not use it at all.

We commend your attention to recent guidance developed by the Article 29 Working Party of the European Union Data Protection Authorities on the consent obligations of the GDPR.[3] Article 29 Working Party also indicates that data controllers should not overly rely on consent due to the burden it places on the user and the risk of "consent fatigue." Moreover, in instances where there is a substantial imbalance of power between the individual and the data controller, consent may not be meaningful and therefore would be an inappropriate basis for data processing. For the majority of data processing at work, the lawful basis cannot and should not be the consent of the employees as it is unlikely that employees will feel able to freely respond to a request to process, or able to refuse without detriment. Similar to public authorities, however, employers may rely on consent under some exceptional circumstances.

The guidelines issued by Article 29 Working Party's on how public authorities can use consent as a basis for processing may be particularly instructive. for example the guidelines provide an overview of the elements of valid consent, which must be "i freely given, ii specific, iii informed, and iv unambiguously indicated. We recommend that the Data Commissioner be empowered to issue guidelines including on effective consent. The development of these guidelines should include an open public consultation.

Section 22 (1) (g) "*only released to a third party only with consent of the data subject*"

[3] GDPR Article 29 guidance

This provision *"third party"* is not clear and needs to be further defined and clarified. It is not clear, for example, how this provision should be read with Section 27 (1)(b)(i) authorized processing of personal data for the purpose of performance of a contract, or Section 27(1)(b)(ii) compliance with any legal obligation to which the data controller is subject.

Section 25 (2) (e) *"The collection from another source would not prejudice the interests of the data subject"*

The term "prejudice" is ambiguous and requires further elaboration. We recommend deletion of this clause. Left as is, this provision would create a large loophole which could be used by data controllers to evade the protections and obligations enshrined in this bill.

Section 27: Lawful processing of personal data.

Section 27 Lawful processing of personal data.
Section 27 (1) *"A data controller or data processor shall not process personal data unless-"*
27 (1) (a) *"the data subject consents to the processing for one or more specified purposes"*

The current language in this provision, that consent can be made for processing of "one or more" purposes, may lead users to not fully understand all of the purposes of processing that they are consenting to. Indeed, companies or the government could use this provision to obtain consent for a broad purpose, which would lead to the user being surprised when the data controller takes a certain action. We would recommend the deletion of "for one or more specified purposes" and just leave this provision as "the data subject consents to the processing." The GDPR article 29 states that consent is required to be "unambiguous" informed, clearly given, and specific.

Section 27 (1) (b) (i) *"For the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract"*

Performance of the contract is a vital basis for processing, not just before a contract is signed but on an ongoing basis. For example, if a user buys groceries on Jumia, the company will likely convey the user's payment details to a third party payment gateway and then provide their address to a third party shipping company. The user should not have to provide consent for each of these additional processing actions, the user expects this to happen when they make their purchase in the first instance, and asking for consent repeatedly in this type of scenario would likely lead to consent fatigue. If performance of the contract is not a lawful basis for processing, it's not clear that many transactions in the digital economy would be lawful. The Consumer Protection Act 46 of 2012 and the Kenya Information and Communications (Consumer Protection) Regulations, 2010, and the Regulation of Sim Card Registration 2015, however provides for lawful processing in the context of a contract or the intention to enter into a contract.

Section 27 (1) (b) (iv) *"for the performance of a task carried out in the public interests or in the exercise of official authority vested in the controller"*

We are concerned that "a task carried out in the public interest" is too ambiguous of a term, and could be used to justify processing actions that do not comport with the rights and interests of users. Is Safaricom business in the public interest? There are legitimate uses of a public interest grounds for processing (e.g., publishing the biographical details of a wanted

criminal), but this provision must be more narrowly constrained. Furthermore, we are also deeply skeptical of the notion of vesting official authority in non-governmental data controllers. If there is a specific use case that the bill is seeking to permit with this provision, we would respectfully recommend articulating that purpose in detail.

Section 27 (1) (b) (v) *"the performance of any task carried out by a public authority".*

We are concerned that this provision would give the government carte blanche to carry out any data processing, providing a loophole for unchecked government surveillance among other potential abuses. Public authorities often have disproportionate power relative to citizens, and therefore consent in many cases may not be appropriate, this does not mean that public authorities should not be subject to other data protection obligations. Specifically, we would recommend amending this section to clarify that all processing performed by public authorities must be subject to privacy and data protection obligations.

Section 27 (1) (b) (vii) *"for the legitimate interests pursued by the data controller or data processor by the third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms of legitimate interests of the data subject;"*

We note that while the concept of "legitimate interest" can be used to process data in a way that does not pose substantial risks to the user, it can also easily be abused by companies. A frequent justification for legitimate interest is to allow for innovation and testing of new products and services. While innovation and testing of new products are important, we believe there are other ways to protect these activities without putting the privacy of users at risk with such an open-ended exemption. When Mozilla seeks to conduct research or test browser features that might reveal sensitive information about users, we utilise several experimentation platforms that require users to opt into tests. For example, users can join the Test Pilot program, which will install new addons with additional browser features. Those addons will often provide Mozilla with additional data to understand users' experience with new features. Alternatively, Mozilla also conducts opt-out tests of new features in cases that represent minimal privacy risk to users and where measuring interactions with new features allows us to improve the product for users.

Given that legitimate interest is a vague concept that can easily be abused at the expense of user data protection rights and interests, we respectfully recommend that legitimate interest be narrowly and specifically defined if it is included. In particular, it would be beneficial for guidance to be developed -- most likely by the DPC after enactment of the data protection law -- articulating how legitimate interest can be used without overriding the rights of the individual.

Section 27 (4) "A *data controller contravenes the provisions of the section*"

27 (4) (1) *"commits an offence and shall, on conviction, be liable to a fine not exceeding five million to imprisonment"*

We propose a stiffer penalty that will provide incentives to data controllers and processors to abide by the provisions of the law. We recommend replacing the maximum fine of five million Kenyan Shillings with 5% of an organization's annual turnover. We believe that strong penalties and a strong, independent regulator are critical to the effectiveness of data protection law.

Section 29 Processing of personal data relating to a child.

Section 29 (1) *"Every data controller or processor shall process personal data of children in a manner that protects and advances the rights and best interest of the child."*

We note that the right to privacy of children is currently protected under the Children Act of 2001, Article 19. We would encourage the Government of Kenya to reconcile this bill with that legislation in order to ensure that there is legal clarity on the data protection rights of children and the obligations on data controllers and processors who process the personal data of children. Additional safeguards must be provided against knowingly marketing, tracking, or profiling children without the consent of their parental guardian.

Section 29 (2) *"A data controller shall incorporate appropriate mechanisms for age verification and parental consent in order to process personal data of children, such mechanisms determined on the basis of –"*

(a) *"Volume of personal data processed"*
(b) *"proportion of such personal data likely to be that of children;"*
(c) *"possibility of harm to children arising out of processing of personal data; and"*
(d) *"such other factors as may be specified by the authority,"*

While, consent is the most important ground for legitimizing data processing activities, the parental consent requirement in this section raises practical questions regarding its implementation.
The EU's GDPR is instructive, it requires data controllers to provide transparent privacy notices in clear, accessible language and a clear affirmative, explicit action in order to provide consent.

We propose further reflection on parental permission. To this end, the DPC should be mandated to provide guidelines on the impact of data protection law on children. Further, in collaboration with stakeholders, the DPC should explore these proposed approaches, particularly those relating to age verification mechanisms because there is a lack of effective technologies to verify that a user is above the age of consent. This may be especially challenging for ISPs and browsers which carry a significant amount of traffic, but otherwise don't have an effective means of restricting that traffic without blocking all traffic entirely.
It would also be helpful to provide additional clarity as to what volume of data or what proportion of personal data likely to be that of children would implicate data controllers or processors under this provision.

Section 29(3) *"The data commissioner may appoint a guardian of the child controller or processor who-"*
29 (3)(a) *"operate commercial websites or onlines services directed at children; or"*
29 (3) (b) *"process large volumes of personal data of children"*

The legal formulation of appointing data controllers and processors is a confusing legal instrument, which does not seem to be required in order to implement the other protections contained in Section 29. We are particularly concerned with any additional primary and secondary liability which might exist for data controllers and processors who are designated as guardians under Subsection 3. The usage of the word "guardian" in this section also does not comport with the common usage of the word guardian or as that term is used in the Children

Act of 2001, and therefore the expectations of parents and users. We would recommend Subsection 3 and Subsection 5 should be deleted in their entirety and that Subsection 4 is amended to read: "Data controllers or processors shall be barred from knowingly profiling, tracking, monitoring, or engaging in targeted marketing directed at children without the consent of the child's parental guardian."

Section 34: Right to Data portability
Section 34 (1) "A *data subject as the right to receive personal data concerning them, which the data subject has provided to a data controller or processor, in a structured, used and machine-readable format*"
Section 34 (2) "A *data subject has the right to transmit the data obtained under sub section (1) to another data controller or processor without any hindrance*"

As one of the world's biggest and oldest open source companies, Mozilla has long been a proponent of open standards and interoperability. We believe that the right to demand all personal data in a "commonly used" machine readable format or transmitted to another service provider with the consent of the individual is essential to strengthening user control and enhancing healthy competition while reducing the costs of innovation.

Section 36 Right to erasure
Section 36 (1) "A *data subject may, subject to exemptions under this Act, request a data controller or processor to-*"
Section 36 (1) (a) "*erase or destroy personal data that the data controller or data processor is no longer authorized to retain, irrelevant, (unnecessary) excessive or obtained unlawfully*"
Section 36 (2) (b) "*Erasure or destruction of such personal data that the data controller is no longer authorized to retain irrelevant (unnecessary), excessive or obtained unlawfully*".

We propose adding **"**unnecessary" to these provisions. Fundamentally, if the information is no longer necessary for the purposes for which it was collected, it should no longer be retained. It is possible to imagine information that is relevant, not excessive, and lawfully collected, but which is no longer necessary for the original purposes. Amending the additional qualification of "unnecessary" would close a loophole that could be exploited to erode the otherwise strong protections of this provision.

Section 37 Security Safeguards of Personal Data

There are many accepted security practices such as multi-factor authentication, security audits, and role-based access control which should be required for the processing of sensitive personal data. As the state of security good practice changes, some of these requirements may also periodically need to be updated. We would recommend that the DPC is empowered, subject to a public consultation process, to periodically update security guidelines for data controllers and processors in accordance with this law. We further recommend that while storing or transmitting sensitive personal data, all data controllers and processors be required to encrypt the data.

Section 37(1) "A *data controller or data processor shall take the necessary steps to secure the integrity and [confidentiality] of personal data in their possession or control through adoption of appropriate reasonable technical and organizational measures to prevent-*"

We propose the addition of confidentiality in this section. Apart from integrity, data controllers and processors must be obligated to safeguard the confidentiality of individuals.

Section 37 (2) (a) *"identity foreseeable internal and external risks to personal data under the person's possession control"*

We believe this is a drafting error and suggest replacing Persons with data controller and processor.

Section 37 (2) (c) *"The pseudonymization and encryption of personal data".*

We recommend amending this provision to read "...encrypt personal data or protect this information with other privacy enhancing techniques or technologies." We believe that all data controllers and processors should take appropriate and reasonable measures to safeguard the data that they have been entrusted with, and pseudonymization can be a powerful tool in some situations, but in many cases this would not be appropriate. For example, any account that must be tied to one's name in order to function. Yet, the bill as currently written seems to require all data to be pseudonymized. We would further note that there is abundant research demonstrating how often pseudonymization can be reversed to re-identify an individual, so we would caution against over reliance on this technique as a safeguard. We would further support an obligation on data controllers and processors to encrypt all sensitive personal data, both in transit and in storage.

Section 38 Notification of breach of security on personal data
Section 38 (1) *"Where there is a breach of security of personal data or there is reasonable ground to believe personal data has been accessed or acquired by unauthorized person the data controller or data processor, within the prescribed period shall-"*
Section 38 (1) (a) *"notify the Data Commissioner"*
Section 38 (4) *"The notification of the data subject shall be in writing and shall be communicated in the prescribed manner."*

We note that there may be breaches that impact very few users, cause minimal harm, or are mitigated by encryption or other remedies. Based on these factors, it might be the case that every breach need not and should not be notified to the data subjects. However, we think that it is important for the DPC to have some periodic visibility into such instances in order to ensure accountability. Data controllers and processors should still be required to log all such breaches, along with their self assessment of the risk, so that periodically the DPC has the opportunity to review. The DPC should also publish clear guidance on the criteria with which to assess harm and risk to the user in order to prevent varying standards of self-assessment. For example, it may be reasonable to categorise those cases where data is encrypted or de-identified and the key or corresponding records (in the case of de-identification) wasn't breached as zero/low risk of harm to data subjects and therefore not requiring follow up action by the DPC.

Where data controllers or processors directly notify their users of a breach or other compromise of their personal data, a copy of the same should be sent to the DPC for review. If the Data Protection Commissioner finds such notice to be insufficient, they should still have the opportunity to order the data controller or processor to take additional action.

We recommend amending this provision to mandate that a record of every data breach (with exceptions for zero/low risk of harm breaches) is maintained by the data controller or processor for periodic review by the DPC. We further recommend a requirement that the DPC issue interim guidelines and procedures on what the "prescribed manner" means in practice within 90 days of the enactment of the Data Protection law, followed by a public consultation

leading to final rules.

Section 38 (5) (d) *"where applicable the identity of the unauthorized person who may have accessed or acquired the data."*

We recommend amending this provision to clarify that the identify of the unauthorized person who may have accessed or acquired the data should be disclosed where available. Attribution of hacks, attacks, and breaches that lead to the unauthorized disclosure of personal data is often very challenging, difficult and time consuming, even for the most well-resourced data controllers and processors. Furthermore, notification of an unauthorized disclosure to affected data subjects, including information about how these users can protect themselves, should not wait for attribution in most cases. This amended language would go a long way to ensuring that notification occurs in a timely manner and provide greater legal clarity to data controllers and processors of what is required in these scenarios. If the government chooses to retain the current language of "*where applicable*" we would recommend additional detail on what situations would and would not be applicable, or requiring the Data Protection Commissioner to issue guidance on the same.

Part V: Grounds for Processing of Sensitive Personal Data

Section 39 Processing of sensitive personal data

We note with concern the discrepancy between the definition of sensitive personal data in the policy and in the text of the bill itself. While we believe the policy's language includes a generally progressive list of what should be considered sensitive personal data, we do believe there are several critical omissions that most users would consider sensitive.
The policy defines sensitive data as:

(a) Racial, ethnic, social origin,
(b) Political opinions or the religious conscious belief, culture dress language or birth,
(c) Gender
(d) Whether the data subject is a member of a trade-union.
(e) Disability
(f) Sexual life or orientation
(g) Pregnancy
(h) Colour
(i) Age
(j) Marital status
(k) Health Status
(l) the commission or alleged commission of any offence by the data subject ,or
(m) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings
(n) Biometrics

We believe this list should replace the definition of sensitive personal data in the bill and should be further amended to include: official or national IDs, passwords, financial data and location information. Financial data for example would have legal and ethical reasons, issues pertaining to personal privacy, or proprietary considerations.

Also, it's unclear what "personal preferences" means in this context. We would recommend omitting this language as it does not provide sufficient legal clarity.

Section 40 (1) *"Without prejudice to section 38, sensitive personal data of a data subject may be processed where-"*

40 (1) (a) *"the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body of a political, philosophical, religious or trade union"*

Political organisations, churches and trade unions collect and process sensitive data, which may be used to implicate an individual's sensitive nature creating potential for personal harm.

We respectfully recommend deletion of this section, or obligating *"foundation, association or any other not-for-profit body of a political, philosophical, religious or trade union"* to comply with all data protection principles and restrictions, including enforcement actions in response to complaints and a stricter regime for certain specified categories of data codified to provide certainty to data controllers and processors.

Section 41 *"Personal data relating to the health of a data subject may only be processed"*

(a) "by or under the responsibility of a professional; or"

(b) "by a person subject to the obligation of professional secrecy under any enactment."

The evolution of new technologies, in particular health related wearables (e.g., the Apple Watch and Fitbit that contain biometric sensors) and other health applications increasingly demanded by users may be precluded by this section as currently written. At the same time, we recognize the rising concerns around how some companies are using health data. We believe that the Data Protection Commissioner should publish guidance in this area, and that explicit consent (and the ability to withdraw consent) should be required to use health data as with other sensitive personal data, but this provision as currently worded is too narrow.

Part VI: Transfer of Personal Data Outside Kenya

Section 22: (1) *"Every data controller or data processor shall ensure that personal data is–*

(h) not transferred outside Kenya, unless there is adequate proof of adequate data protection laws by the recipient country".

Section 44 *Rule as to data centers and servers.*

Section 44: (1) *"Every data controller or data processor shall ensure the storage, on a server or data center located in Kenya of at least one serving copy of personal data to which this act applies.*

Storing a copy of all personal data pertaining to Kenyans in a handful of locations could create a "honey pot" for malicious actors, therefore increasing vulnerability to breach. In comparison, distributing storage of data across a network of servers globally means that there is no concentrated point of attack or single point of failure. Many businesses might find that this mandate would jeopardize the security of the personal data they retain, with implications for users globally, not just in Kenya.

In addition, a requirement to store data locally, or store at least a copy of data locally, introduces potentially higher costs and actual limitations on technology innovation, development, and use. When faced with the mandate to store at least a copy of the data in Kenya, many companies might choose to store only in Kenya to save on costs. Efficient internet routing depends on the network's end-to-end design and dynamic transfer of packets of data. Routing protocols are designed to ensure that these packets travel along the most efficient route between two points. Limiting the routes data can travel ultimately undermines the

efficiency and potentially the integrity of internet traffic.

Other small and medium sized global companies, in particular, might find that this requirement increases storage costs significantly, or compromise the security of their services, and might choose to close off their services to Kenyan users. This would be a loss to the vibrancy of the Kenyan digital ecosystem, and eventually, this loss of choice will hurt the end user.

Moreover, any move to require data to be located in Kenya would not only set a dangerous example for other countries, but also other countries would likely reciprocate in kind, requiring Kenyan companies to store data in their jurisdictional borders, in turn introducing a heavy burden on Kenyan companies looking to have global presence. Rather than ease the challenge of gaining lawful access for investigative purposes to personal data stored abroad, this state of affairs would exacerbate challenges for Kenyan LEAs.

A requirement to store data in the country will likely create a conflict of laws situation for multinational companies. U.S. law, for example, would still effectively limit companies from disclosing many kinds of user data to foreign law enforcement authorities without a US warrant or subpoena. A similar situation is likely to hold for European companies, as per GDPR Article 48. Localisation does not, and should not, by itself do away with these procedural safeguards and cannot override foreign laws and treaties governing data flows.

There are also many benefits to allowing the free flow of data across borders. If the EU were to determine that Kenya's data protection law offered "adequate" protections on par with the GDPR, data and services could flow freely between Europe and Kenya. This would enable Kenyan companies to much more easily enter the European market and all other markets that have received adequacy from the EU. At the same time, having a substantially similar data protection regime would make it easier for European, American and other foreign companies to invest and process data in Kenya, allowing greater expansion into the Kenyan market without the costs of designing and maintaining a separate system for data processed in Kenya.

While the EU has an established mechanism for recognizing whether another country has an adequate level of data protection, this mechanism in the Kenyan context is not yet established. While we recognize the interest of the government in ensuring that Kenyan data is not transferred to countries with insufficient data protection regimes, we would respectfully recommend articulating a procedure for assessing data protection adequacy in this legislation.

Section 44 (2) *"The Cabinet Secretary shall prescribe, based on grounds of strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data center located in Kenya"*

We acknowledge that certain categories of personal data may need to be mandatorily stored within the country, with restricted data flows, due to the strategic and security interests at play. It is reasonable therefore for defence data, for example, to be stored exclusively in Kenya as is current practice. However, Section 44(2) of the bill leaves the definition of critical personal data entirely open to Government discretion and does not elucidate what such categories might be, nor any parameters to circumscribe this discretion. Since mandating data storage in Kenya generally amplifies the concerns of routing inefficiencies, increased costs, and security risks, this wide discretion is concerning.

We recommend that categories of critical personal data that are currently localised in Kenya

for strategic or security reasons should be clearly stated. The open ended mandate to the government to notify further categories should be removed.

Section 44(3) "*Cross-border processing of sensitive personal data is prohibited*"

In addition to the concerns raised above, we recognize the needs and compelling interests of both private and public data controllers and processors to process sensitive personal data outside of Kenya. For example, financial institutions (whether banks or public authorities) transfer financial information to check for fraud and terrorist financing, for example. This provision as currently written could be read to preclude Kenya's participation in the SWIFT network, which would be gravely detrimental to Kenya's financial sector and economic standing in the world.

We respectfully recommend deletion of section 44.

Part VII: Exemptions to Data Protection Requirements

Most international data protection regimes contemplate several exemptions to certain data protection requirements. Exemptions however mean that the constitutional right to privacy is limited. While we believe that there are several such grounds that should be enshrined in the data protection law, these exemptions must meet the threshold provided for in article 24 of the constitution of Kenya, 2010, which provides for the "*limitations of rights and fundamental freedoms*" and no statue can impose any other limitations. Furthermore, consent of the user should be the preferred route in most cases. Events, that may amount to limitations to users' rights should only be permitted if in pursuance of a *legitimate* aim, proportionate, narrow, and in compliance with Article 24 of the Constitution. Limitations must specify the privacy aspects that would be limited. The principles of data protection must still apply even under such limitations.

We are concerned that some of the exceptions provided in the Bill do not appear to satisfy these proportionality tests. We are particularly concerned about the following clauses:

Section 4(2)(a): Application This Act shall not apply to –

(a) "the exchange of information between government departments and public sector agencies where such exchange is required on a need- to-know basis;"

While we recognize that there may be legitimate reasons for various parts of the government to share information with each other (e.g., to mitigate a terrorist threat), we also believe that this provision is quite broadly worded. In addition to requiring information to be shared on a need-to-know basis, we would further recommend requiring this processing to be necessary and proportionate. Furthermore, while the obligation to seek consent may not apply in these scenarios, public authorities should still always be bound by the other principles of data protection including purpose limitation, collection limitation, security safeguards, etc.

Section 25 Collection of Personal Data

Section 25 (2) *"Despite Subsection (1) personal data may be collected indirectly where-*

(e) the collection from another source would not prejudice the interests of the data subject

(f) collection of data from another source is necessary-

(f) (i) For Prevention, detection, investigation, prosecution and punishment of crime

(f) (v) in the interest of national security"

Section 47 (2)" *The processing of personal data is exempt from the provisions of this Act if-*

47(2) (a) exemption is necessary for national security or public order
47 (2) (b) disclosure of required by or under any written law or by an order of the court
47 (2) (c) the prevention or detection of crime
47 (2) (d) the apprehension of prosecution of an offender: or
47 (2) (e) the assessment of collection of a tax or duty or an imposition of a similar nature"

These exemptions for the purposes of investigating a crime, prosecution of crime or for any other purposes related to maintaining "*national security*" must be understood as exemptions from seeking user consent, not from all data protection requirements. Where legal obligations require the collection of data from an indirect source, the enabling legal provisions provide a procedure for such a collection e.g. a court order. Allowing other government entities to access information provides a route to circumvent normal procedures. Exempting entire law enforcement and tax collection agencies from all data protection requirements is untenable and in conflict with the Article 31 of the constitution of Kenya 2010. It also undermines Kenya's obligations under international law.

In addition, all law enforcement, intelligence, and other national security agencies must be bound by requirements around data security, purpose limitation, collection limitation, the right to rectify, the right to erasure, etc. Given the disproportionate power of the State vis-a-vis the individual, the unparalleled access to personal data available to the State, and the substantial interference and invasion into the private lives of individuals that the State is capable of, the authority of the State must be prescribed in law and additional protections for individual security and privacy required.

These clauses must be clear, limited, construed, in the public interest, and enshrined in law. Moreover, all exemptions should be understood as an exemption to seek the user's consent to store, access, analyze, or process user data, not as a blanket exemption from all data protection obligations. There is a need for careful analysis to ensure that any exemptions are narrowly defined and describe specific permitted activities. All data processing must also be necessary and proportionate.

Section 49: Research, history and statistics
Section 49 (1) *"The further processing of personal data for a research purpose in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained".*

We believe this provision could be potentially abused by data controllers and processors. It is easy to imagine a company wishing to engage in big data analytics simply labeling their processing action as "research" in order to evade the otherwise strong protections of this bill. The same could be said for government surveillance. We recommend clear definitions and limiting scope for research purposes that is aimed at or culminate in commercial exploitation.

Conclusion

In Kenya's new constitution 2010, the government took important action to recognize and protect the right to privacy in Article 31. The data protection legislation under discussion today represents an historic next step in the cause of protecting Kenyans, especially in the face of new technological developments. We commend the Government of Kenya for the thoughtful and thorough framework, which we believe with some amendments has the potential to be a model to all African nations.

We look forward to continuing to work with the Ministry and the Task Force as you further develop Kenya's first data protection bill.

Thank you for your consideration of our submission.

For any further questions please consult Mozilla Policy Advisor Alice Munyua (amunyua@mozilla.com).

Respectfully submitted by:

Alice Munyua
Policy Advisor
Mozilla Corporation

Jochai Ben-Avie
Senior Global Policy Manager
Mozilla Corporation