For attention:

Mr. Jerome Ochieng

Principal Secretary, ICT & Innovation

Ministry of Information, Technology and Communication

pdp@information.go.ke; pdp@ca.go.ke

Submission by:

Research ICT Africa: Digital Policy Project

Unit 409, Old Castle Brewery

Beach Road, Cape Town, South Africa

Contact person: avanderspuy@researchictafrica.net

18 September 2018

IN RE: Comments on *Policy and Regulatory Framework for Data Protection* in Kenya

This submission is made in response to a call for comments on the *Policy and Regulatory Framework on Privacy and Data Protection by the Task Force on Data Protection*, which was constituted by the Cabinet Secretary, Ministry of ICT, in May 2018.

Research ICT Africa welcomes the effort by the Government of Kenya to give effect to informational privacy guaranteed in Article 31(c) and (d) of the *Constitution of Kenya*, and also appreciates the opportunity for public consultation on the proposed *Privacy and Data Protection Policy* and *Data Protection Bill 2018*.

Data is inherently important to sustainable development, economic growth and the future of African countries more generally.[1] But in today's increasingly digital societies, individuals tend to have limited control over how their data is collected, stored, used, and/or disseminated. While citizens might benefit from the convenience that is often the consequence of wide-ranging data processing activities, inherent risks related to increased data processing include increased grounds for discrimination, the deepening of existing inequalities, and greater opportunity for state, social and private surveillance.[2]

While there appears to be general global consensus about the need for data protection, in practice there are vast differences between regional and national interpretation and implementation of data protection principles. In North and West Africa, for example, ten countries have adopted data protection frameworks between 2013 and 2018. Some argue that this is as a result of the existence of a regional network of data protection authorities supporting cooperation and training initiatives where data protection is concerned.[3]

Despite this development, less than a quarter of all African countries have data protection frameworks in place today.[4] We believe Kenya can set a positive example for East Africa by developing a data protection framework that puts people at the centre of the digital economy. Findings from Research ICT Africa's 2017 *After Access Survey* show that although Kenya has a growing Internet penetration rate of around 30%, large numbers of people remain offline due to demand-side constraints such as lack of awareness of the Internet (27%), the affordability of devices (25%), the cost/affordability of services (25%), and a lack of interest in what the Internet has to offer (26%). The drivers of Internet adoption is education and the correlating factor of income.[5]

Our *After Access* work has repeatedly underlined the fact that people who are the most marginalised in societies are also the most susceptible or vulnerable to having their human rights infringed. This is due to twin challenges related to marginalised people tending to lack relevant awareness of how to keep their data safe and secure, along with the absence of knowledge or skills to safeguard them both offline and online.[6] Working towards the establishment of robust data protection frameworks that place people – including marginalised people – at the centre is therefore crucial for all developing countries.

Data protection frameworks have been in place for a while, but have come under increasing strain as a result of the fast pace of technological advancement – including developments related to Artificial

---

[1] c.f. UNGA. *Resolution adopted by the General Assembly on 25 September 2015: Transforming our world: the 2030 Agenda for Sustainable Development* (A/Res/70/1). (2015b, October 21). New York: UNGA. www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.
[2] Shephard, N. (2016). *Big data and sexual surveillance (APC issue paper).* Johannesburg: APC. www.apc.org/en/system/files/BigDataSexualSurveillance_0.pdf.
[3] Global Partners Digital (2018). *Travel Guide to the Digital World: Data protection for human rights defenders.* https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf.
[4] The Internet Society (2018) The Internet Society and African Union Commission Launch Personal Data Protections Guidelines for Africa https://www.internetsociety.org/blog/2018/05/the-internet-society-and-african-union-commission-launch-personal-data-protections-guidelines-for-africa/
[5] Research ICT Africa (2018). *After Access highlights.* https://researchictafrica.net/2018/01/15/after-access-highlights-using-evidence-from-the-global-south-to-reshape-our-digital-future/.
[6] Research ICT Africa, 2018, *ibid.*

Intelligence (AI) and the Internet of Things (IoT). Among other things, these developments have made it more difficult to obtain meaningful user content and to enforce user rights, especially where global digital giants are concerned.[7]

Besides the importance of safeguarding the data of Kenyans who are yet to come online, Kenya's draft *Privacy and Data Protection Policy* and *Data Protection Bill* are also timely considering the fact that data protection in Kenya is currently only covered in part through a mélange of separate and mainly sectoral policies in diverse sectors.[8] We believe the proposed legislative changes can introduce more clarity and holistic data protection for Kenyans than the current situation has been able to do. Such a framework needs to be flexible enough, however, to meet the inevitable data demands that will become increasingly prevalent as evolving technology such as AI and IoT become more integral to everyday life – also in Kenya. The current framework, therefore, needs to be sufficiently flexible and future-proof as far as is reasonably possible to allow for the inevitability of new challenges related to technological change.

Besides these comments on the general spirit and purpose of the new data protection framework, we believe it will only be beneficial to Kenyans if it also serves to protect Kenyans' data adequately and in a practical manner. To do so, it is important that some aspects of the proposed framework be re-evaluated. These include:

a) Principles, rights and exceptions

We note that the *Data Protection Bill* sets out principles of data protection that largely mirror international standards (c.f. Part IV of the Bill). Moreover, the *Bill* provides for data subjects' rights and elaborate general grounds for data processing. We commend the Task Force for these provisions, and hope these efforts will enable Kenya to continue putting its citizens and their rights first where the growing digital economy is concerned.

The *Data Protection Bill* seeks to give effect to Article 31 of the *Constitution of Kenya*, which protects a person's private affairs as well as their communications. This right is particularly important in today's digitalised world where individuals tend to have limited control over how their data is collected, stored, used and disseminated. While citizens do benefit from data processing activities – often in terms of convenience factors – inherent risks related to increased data processing include increased grounds for discrimination, the deepening of existing inequalities, and greater opportunity for state, social and private sector surveillance. We therefore recommend that, first and foremost, the *Privacy and Data Protection Policy* and *Data Protection Bill* safeguard the right to privacy of the person across all of its provisions through: being the primary and overarching law on privacy and data protection; avoiding provisions that

[7] Global Partners Digital (2018), *ibid.*
[8] Kumar, S. & Wingfield, R. (2018). *Data protection on the ground (#1): Kenya's draft Bill.* Global Partners Digital. https://www.gp-digital.org/data-protection-on-the-ground-1-kenyas-draft-bill/.

make some data processing practices in public offices immune from application of the law; and avoiding broad exemptions of public offices from application of the law.

We acknowledge the fact that in specific situations there may be tension between privacy and certain state obligations such as the provision of security and the maintenance of public order or safety. In those events, exceptions that may amount to limitations to human rights should be permitted if in pursuance of a legitimate aim, proportionate, narrow and in compliance with Article 24 of the *Constitution of Kenya*. Further, limitations should specify the aspect of privacy (e.g. data subjects' right to access their own data) that is to be limited and, even under such limitations, the principles of data protection still apply.

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 provisions on exceptions on grounds such as national security (clause 3), what is "reasonably practicable" for a data controlled (clause 26), and the assessment of taxes (clause 47), for instance.

b) Institutional capacity and independence

While having principles and grounds in place is an important first step, we also encourage the Task Force to ensure that adequate and reasonable provision is made for the implementation and enforcement of principles and grounds. Without tangible efforts at enforcing data subjects' rights, including capable, resourced and trained institutions, the principles and grounds will do mere lip service to Kenyans' human rights online and offline.

While the Bill's proposed enforcement through the office of the data protection commissioner is welcomed, we also believe it important to ensure the independence and strengthen the institutional capacity of this office. Independence should be facilitated at various stages, including at the appointment of the commissioner where a more robust and inclusive mechanism should be applied; financing of the office; in carrying out its functions where the role of the executive should be minimal; and in potential removal of the commissioner which should be done as with other state officers under the *Constitution of Kenya*.

c) Protecting innovation and promoting healthy digital competition

Kenya has a nascent data economy with big private sector actors as well as small and medium enterprises (SMEs) conducting data processing activities. Once a new data protection framework is established in the country, larger players, as well as those already regulated in other sectors, will likely have ease of compliance as compared to smaller actors.

As all of these actors play important roles in the country's digital transformation, we recommend that the Task Force develop mechanisms for assisting SMEs to understand the changing legal framework and to develop their capacity to provide the highest protection for personal data in their custody. Similarly, we recommend that platforms that collect, store, use, and/or disseminate Kenyans' data should be obliged to enable the portability of anonymised bulk data to others for a reasonable fee and in an accessible (or interoperable) manner. Such data-sharing requirements could be calibrated to firms' size: the bigger platforms are, the more they have to share at lower costs.

Some related suggestions for the Task Force to consider include:

- having different classes in the registration of data processors and controllers;
- empowering the commissioner in partnership with stakeholders to facilitate the training and continued education of SMEs;
- developing codes and standards for SMEs; and
- designing graduated penalties depending on the size of the data processor/controller.

d) Penalties and remedies

The Bill proposes the imposition of criminal liability for data-related offences (e.g. data controllers' failure to adequately protect data). Fines and jail terms are the proposed consequences of contraventions (c.f. clauses 23, 38). While this may have the intended deterrent effect against unlawful processing of data, we believe this is overly severe.

In addition, the provisions fail to serve the purpose of providing sufficient remedies for the victims of data offences. For instance, if a person's sensitive health data was disclosed at their place of work, criminal sanctions against their employer may not necessarily compensate the damage caused to their person. While keeping our recommendation about not unduly imposing criminal sanctions in mind, we therefore propose different and more targeted sanctions which could involve graduated administrative fines, enforcement notices and direct liability for culpable directors of data processors and controllers.

e) Opening data for research and innovation

Kenya's proposed policy on data protection situates the country as an emerging data economy and predicts increased data processing activities. Indeed, the framework envisages use of data for research and provides for anonymisation and pseudonymisation for artistic, academic, research and public interest purposes.

From observing global trends as well as the Kenyan ICT sector, it is highly probable that large digital players will continue to leverage data to gain more market share in adjacent markets, and to therefore control or even stifle innovation. As noted in the previous point, we therefore recommend that the proposed law obliges platforms to share anonymised bulk data. This will not only create an a more open data economy, but will also foster a contributory model where data is not used to suppress competition but to enhance human development.

Conclusion

Research ICT Africa believes that the proposed framework has the potential to safeguard the fundamental rights of individuals if the necessary modifications as suggested in this submission are made. We believe this framework can go a long way to creating the safe and trusted environment required to get Kenyans universally online and optimally utilising the Internet for their well-being and the nation's development.

Along with our colleagues across Africa, we look forward to the realisation of a data protection framework in Kenya that affords the highest protection of privacy and provides strong good practices for the broader region.

About Research ICT Africa

RIA has over 15 years of consistent experience in research on information and communication technology (ICT) policy and regulation. It helps to facilitate evidence-based and informed policymaking for improved access, use and application of ICTs for social development and economic growth in Africa.[9]

RIA's Africa Digital Policy Project focuses specifically on cyberpolicy challenges for Sub-Saharan Africa. Like RIA's other work, the Project provides African stakeholders with the information and analysis required to develop innovative and appropriate policies better able to address the challenges of sustainable development on the continent. It thereby facilitates evidence-based and informed policymaking for supporting the development of an Internet that is free (based on and supportive of human rights), trusted (based on sound cybersecurity measures), and innovative (based on enabling policy environments).

Contact details:

Anri van der Spuy (avanderspuy@researchictafrica.net)
Research ICT Africa: Digital Policy Project

[9] Read more about RIA's work here.

Unit 409, Old Castle Brewery
Beach Road, Cape Town, South Africa