**Request for Feedback: 5-Year Reflections on Kenya's Data Protection Act.**

**Dear Listers,**

As part of our ongoing efforts to assess the effectiveness and impact of Kenya's Data Protection Act (2019) over the past five years and in anticipation of the NADPA Conference being held from 7 - 9 May 2024, we are reaching out to gather your valuable insights and reflections. To this end, KICTANet will be moderating an online discussion on the KICTANet mailing list from Monday 29 April 2024 - Friday 3 May 2024. We want to draw special attention to the contributions of the Data Governance and Emerging Technologies Working Group on the ICT legislative reform process and in particular the recommendations on data governance.

To chart the progress, challenges, and considerations for the future of data protection in Kenya, KICTANet shall be exploring the following topics over the course of next week through targeted daily questions for your reflections.

**TOPICS:**

**A. Day 1: Legal Framework on Data Protection**

**B. Day 2: Data Controllers & Processors**

**C. Day 3: Data Subjects’ Rights**

**D. Day 4: Emerging Issues and Best Practices**

**E. Day 5: Recommendations and Shaping the Future.**

Please feel free to respond directly to this email with your insights. Alternatively, you can reach out to Linda Gichohi (lgichohi@kictanet.or.ke) if you have any questions or additional comments.

Thank you for your time and participation.

**Day 1: Legal Framework on Data Protection**

1. **What areas of Kenya's legal and policy framework on data protection require improvement or updating? Please provide supporting justification/rationale.**
2. **Please provide three (3) recommendations for amendments to the Data Protection Act, and its attendant regulations.**

**Proposed Changes**

* We need a policy of **child online protection** and **data privacy** protection, especially for tech organizations in child online protection.
* The right to forget/forgotten should be expressly stated.
* **Enforcement**: There are concerns regarding the limited **capacity** of the Office of the Data Protection Commissioner (ODPC) to effectively enforce the Act. Strengthening the ODPC's resources and enforcement capabilities is crucial.
* **Public Awareness:** Public understanding of data protection rights and responsibilities remains relatively low. Increased public awareness campaigns and educational initiatives are essential.
* **Cross-border Data Flows**: The current framework may not adequately address the complexities of data transfer across borders. Exploring best practices and potentially updating regulations to manage this is important.
* We need to **review the jurisprudence** from the ODPC to determine whether it has the capacity to regulate tech giants such as OpenAI, Glovo, Uber, and other emerging technologies. Collaborative efforts with the other stakeholders such as the Competition Authority should be favored. Attached [Online-Food-and-Groceries-Delivery-Platforms-Market-Study.pdf](file:///C%3A%5CUsers%5CADMIN%5CDownloads%5COnline-Food-and-Groceries-Delivery-Platforms-Market-Study.pdf) is a report on the challenges that consumers face on the digital food and grocery applications such as Glovo.
* Page 906: ...
	+ "**data subject**" means an identified or identifiable natural person who is the OWNER AND subject of personal data.
* 24. (4) Where a data controller or a data processor is a public body, DATA PROTECTION OFFICERS WILL BE DESIGNATED, TAKING INTO ACCOUNT THEIR ORGANIZATIONAL STRUCTURES AND SCOPE OF COVERAGE ...
* 24 (6) A data controller or data processor shall publish the contact details of the data protection officer on the ORGANISATION'S WEBSITE AND COMMUNICATE THEM TO THE DATA COMMISSIONER ..

 **Proposed Recommendations for Amendments:**

* Increased Fines: Consider raising the maximum fines for data breaches and non-compliance to create a stronger deterrent effect.
* Mandatory Data Breach Notification: Implement a mandatory requirement for data controllers to notify individuals and relevant authorities in case of significant data breaches.
* Clarification on Exemptions: Provide clearer definitions and limitations on exemptions for national security or other legitimate purposes to ensure they are not misused.
* The daily collection of private data at security desks without any oversight, regulation, or assurance of confidentiality and privacy may be a violation of Section 28.
* A clause that requires the data commissioner to prohibit or provide guidance on the collection, storage, and dissemination of personal data by public and private entities (e.g. banks, service centres, public departments, etc) to minimize misuse, ensure consent, and enhance protection of citizen data.
* A clause that would require higher levels of data protection on public digital assets (e.g. websites, social media accounts) including encrypted websites, etc.
* A clause that incorporates sanctions against data protection controllers and officers who do not take required measures to protect data on public assets (digital, physical, etc).

**Day 2: Data Controllers and Processors**

1. **In your opinion, what has been the key impact (positive/negative) of the Data Protection Act, 2019, on state and private entities’ organizational policies, procedures, practices, and compliance levels from 2020 to date?**
2. **Poll:**[**Do you believe that the penalties imposed on organizations for data breaches or non-compliance are sufficient to deter future violations?**](https://www.livepolls.app/result/6622dd8c0d1d3f4c690d6c01)
* In addition to multinational entities, It may be helpful to include primarily local entities - commercial, NGOs and governmental organizations often have data protection practices that are weak where OPDC may have more ability to improve practices.
* A foreign policy objective should be to enable some harmonization in
data protection policies, both to enable foreign companies and citizens
to safely store their data in Kenya.
* A foreign policy objective to enable storing and use of data originating in Kenya elsewhere.
* Recognizing other places where harmonization has been done, and for what types of data would be useful.
* Trafficking of person and data privacy
* Counter-trafficking actors who provide protection and assistance services to trafficked persons are likely to gather and have access to significant amounts of personal data. Therefore, it is important to have a data protection framework in place to safely and securely share data relating to human trafficking.

**Impact of the Data Protection Act (2019)**

**Positives:**

* **Increased awareness of data privacy:** The Act has undoubtedly raised awareness among organizations about the importance of data privacy and the rights of individuals. This has led to a more responsible approach to data collection and usage.
* **Improved data security practices:** Many organizations have implemented stricter data security measures to comply with the Act's requirements. This helps to minimize the risk of data breaches.
* **Standardized data protection practices:** The Act has provided a clear framework for data protection, which has helped to standardize practices across different sectors.

**Negatives:**

* **Compliance burden for some organizations:** The Act's requirements can be quite complex, especially for smaller organizations. This has created a compliance burden for some entities.
* **Limited enforcement capacity:** There are concerns that the current enforcement capacity may not be enough to deter all potential violations.

**Poll: Adequacy of Penalties**

* I voted **"No"** in the poll regarding the sufficiency of penalties. While the Act outlines penalties, their actual enforcement might be a deterrent factor. Perhaps stronger enforcement mechanisms alongside the current penalties could be more effective.

**Day 3: Data Subject Rights****.**

1.        **Have you experienced any changes in the way state/non-state organizations handle your personal data since the implementation of the Data Protection Act, 2019?**

**Data subject rights.**

Changes in Data Handling:

* **Increased transparency**: Some organizations are now more transparent about the data they collect, how they use it, and with whom they share it. This often involves providing privacy policies that are easier to understand.
* **Opt-in mechanisms:** I've noticed a rise in organizations offering opt-in mechanisms for data collection and marketing communications. This allows individuals more control over their data.
* **Data access requests:** While not widespread yet, I'm aware of instances where individuals have requested access to their personal data held by organizations. This demonstrates an increased awareness of data subject rights.
* There is increasing awareness on the need to protect personally identifiable information eg; Consent for taking photos at a public event.
* We have seen increased use of consent for taking photos in educational institutions to protect students' privacy. There is also parental consent, where educational institutions seek consent from parents to process their children's data. In this case, appointing a DPO in state and non-state institutions should be encouraged.

**Day 4: Emerging Issues and Best Practices.**

2.  **What are some international best practices or benchmarks in data protection regulation and enforcement that the ODPC should consider emulating?**

3.   **What recent technological advancement or practice do you believe presents the greatest data protection and privacy opportunity in Kenya?**

* The fines should be reconsidered to cater to the grassroots institutions that may be in breach and lack the financial capability or capacity to pay the fines. We need to think about such scenarios, thus the need for more awareness even in the grassroots.
* The next steps should be massive awareness creation. There is a great need of awareness to be created before we can start emphasizing on punitive actions as a deterrent. We should not run too fast and leave the ball behind as we are accustomed to.
* Regarding the gender aspect, More Kenyan males than females online, meaning the data and information produced may be gender biased. The Afro-Feminist Perspectives on Data Governance and Advancing Data Justice in Africa session – noted the 6 pillars of data justice: power, equity, access, identity, participation, and knowledge which is crucial.

**International Best Practices**

* The Kenyan Data Protection Act is a positive step, but there's room for improvement. Here are some international best practices the ODPC could consider:
* Stronger enforcement mechanisms: Examples include dedicated data protection authorities with investigative powers and the ability to impose significant fines.
* Data portability rights: This allows individuals to easily transfer their data between different service providers.
* Right to be forgotten: This grants individuals the right to request the erasure of their personal data under certain circumstances.

**Emerging Technologies and Data Protection**

* The rise of Artificial Intelligence (AI) presents both opportunities and challenges for data protection. On the positive side, AI can be used to develop more secure data storage and access control systems. However, AI algorithms can also be biased and lead to discriminatory outcomes. Therefore, it's crucial to develop robust data protection frameworks that address these challenges.
* With respect to Technology, AI can help especially using local languages to create more awareness (pin yako siri yako kind of approach).
* Regarding the AI aspect, there should be some policies regarding the use of data that will train AI. For example, in the case of local languages, which data will be used? If data by local language content creators is used, will they be compensated? *Many African languages are poorly resourced, some are also endangered.
Language data should be considered a public good as it can enable use of
AI in many settings.  It does also enable easier surveillance of people
that use that language.  There does not seem to be a government policy
for local languages - even materials for school curricular such as
standard texts and dictionaries are few.  Use of local languages at
county level is probably the easiest place to start as there would  be a
sufficient concentration of active language users.  Languages do divide,
but they also enable diversity in culture and approaches to problem
solving.  While the ODPC has a role to play, probably the main
governmental actor is the Ministry of Sports, Culture and National
Heritage.  The greatest widespread use of local languages is on radio.*
* The best technology advancement could be privacy-enhancing technology(PET), which can enhance the utility of the data while simultaneously fulfilling the entity's key data protection obligations. In that case, the use of privacy by design could be embedded into the design specifications of various technologies, including the adoption of PETs such as homomorphic encryption.