**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.