**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**

**Proposed Changes**

1. We need policy of **child online protection** and **data privacy** protection especially for tech organizations in child online protection
2. **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.
3. **Public Awareness:** Public understanding of data protection rights and responsibilities remains relatively low. Increased public awareness campaigns and educational initiatives are essential.
4. **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.
5. 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.
6. Page 906: ...

"**data subject**" means an identified or identifiable natural person who is the OWNER AND subject of personal data.

1. 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 ...
2. 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:**

1. Increased Fines: Consider raising the maximum fines for data breaches and non-compliance to create a stronger deterrent effect.
2. Mandatory Data Breach Notification: Implement a mandatory requirement for data controllers to notify individuals and relevant authorities in case of significant data breaches.
3. Clarification on Exemptions: Provide clearer definitions and limitations on exemptions for national security or other legitimate purposes to ensure they are not misused.
4. 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.
5. 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.
6. A clause that would require higher levels of data protection on public digital assets (e.g. websites, social media accounts) including encrypted websites, etc.
7. 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).