1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

6 January 2025

Office of Data Protection Commissioner (ODPC)
Britam Towers, 13th Floor
P.O Box 30920-00100 G.P.O
Nairobi

To the Data Protection Commissioner and all the staff concerned,

Comments on the Draft Data Sharing Code, 2024

The Future of Privacy Forum (FPF) is grateful for the opportunity to provide comments on the draft Data Sharing Code, 2024. FPF is a global non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

FPF's Comments

FPF's comments on the draft Data Sharing Code are set out in **Annex 1** for your kind consideration.

We welcome the opportunity for future engagement with the ODPC on the draft Data Sharing Code. If you have any questions on, or responses to, any of the comments set out below, or if we may be of any further assistance in the development of the draft Data Sharing Code, please do not hesitate to contact Mercy King'ori (mkingori@fpf.org). Thank you.

Yours sincerely,
Mercy King'ori
Policy Manager - Africa
Future of Privacy Forum

Annex 1

S/No.	Section of the Code	Provisions of the Code	Proposed Amendment	Rationale for Amendment recommendation
2.	**2.1**	Data recipients should not attempt to reidentify deidentified data.	We recommend clarifying conditions and thresholds to be met where data reidentification may be permitted while maintaining the strict legal framework on reidentification. For instance, legal bases for reidentification, if justified, may include: to protect the vital interests of the data subject, where it is a legal obligation to identify a data subject or where a data subject consents. Even where a lawful ground for reidentification exists, the Code should include conditions that must be met before reidentification can be carried out, such as alignment with	An entity may be engaging another for the purpose of reidentification services to fulfil a legal obligation such as fraud prevention and detection. Therefore, having clear criteria for reidentification will ensure that such legal obligations can be met without uncertainty.

			the principles of necessity and proportionality.	
3.	**3.1.1**	This section requires an organization to clearly explain the legal basis for sharing data and provides specific guidance on measures to be taken by an organization relying on consent for data sharing purposes.	We recommend providing similar guidance where an organization relies on the other legal bases provided for under Section 30(b) of the Data Protection Act, 2019.	This will provide clarity on measures that an entity should take into account when relying on the different legal bases during data sharing. Currently, a common data sharing misconception is that consent is the sole legal basis for data sharing. However, the law provides several grounds for data sharing that would be appropriate in cases where it is not possible for the data subject to provide genuine consent in the given circumstances.
3.	**3.3**	Responsibilities of the transferring entities.	We recommend clarifying the term "transferring entities" by providing a different term to represent such entities. A suggested term for entities sharing personal data could be "primary entity".	The definition of a "transferring entity" under Regulation 39(c) of the Data Protection (General) Regulations, 2021 implies that data sharing entities under consideration in the Code are those that transfer personal data ***out*** of the country. However, the scope of data sharing under the draft Code also includes data

			The term "primary entity" refers to "the entity initially responsible for the custody and provision of personal data to another party."	sharing ***within*** the country.
5.	**5.10**	Data controllers and processors transferring personal data outside Kenya will be required to notify the ODPC of the transfer.	We recommend clarifying whether such notification relates to all or some personal data transfers. Specifically, we recommend specifying the categories of transfers that will be subject to such notification, as well as providing timelines for such notification. For example, the ODPC may establish explicit criteria for transferring personal data to non-adequate jurisdictions as well as	Specific transfer notifications in some cases as well as emphasis on documentation over routine notification will ensure administrative efficiency and legal certainty as broad notification requirements for every transfer will add significant compliance burdens on controllers and processors.

			procedures for notification. Additionally, the Code could emphasize requirements regarding documenting data transfers that can be provided by controllers or processors upon request by the ODPC.	
5.	**5.4**	The Code mandates that data sharing be based on the data subject's consent.	We recommend acknowledgment of other grounds for transferring personal data out of the country already provided under the Data Protection Act and the General Regulations, in addition to consent.	Regulation 40 of the General Regulations provides for other grounds for cross-border data transfers. We recommend aligning this section of the Code with the General Regulations to ensure lawful transfers of personal data where consent may not be the most appropriate ground for such transfers. For example, consent may not be the appropriate legal basis where a telecommunications provider shares network usage data with a cybersecurity

				firm to mitigate potential data breaches or cyberattacks. Legitimate interest may be appropriate in this case because such data sharing safeguards critical infrastructure and data security, providing direct benefits to both the company and its customers.
5	**5.5**	The Code requires controllers and processors to take all reasonable technical, legal and organizational measures, including contractual arrangements, to prevent unlawful international transfers or governmental access to personal data held in Kenya.	We recommend clarifying the "technical, legal, and organizational measures" by stipulating specific examples and aligning them with international standards. Additionally, we recommend briefly clarifying the difference between "unlawful international transfers" and governmental access to data, with guidance on	Detailed definitions of these terms will reduce ambiguity and support consistent compliance for data controllers and processors.

			permissible and impermissible scenarios.	