



The Gap in Kenyan based IPDTs: Adequacy Considerations?

by Amrit Labharam and Michael Butera



Strathmore University
*Centre for Intellectual Property and
Information Technology Law*

EXECUTIVE SUMMARY

Key findings:

Kenya's Data Protection Act (Act No. 24 of 2019) includes provisions that regulate International Personal Data Transfers (IPDTs). Part VI of the Data Protection Act (DPA) states that IPDTs may be conducted with foreign jurisdictions with commensurate data protection frameworks. However, the DPA does not explicitly define the evaluation criteria for these foreign data protection frameworks, making IPDTs non-compliant under Part VI.

Evaluation criteria for foreign jurisdiction's data transfer laws (the 13 principles listed in this brief) will aide with DPA compliance and provide the Office of the Data Protection Commissioner (ODPC) a basis for approving, prohibiting, suspending or subjecting IPDTs to such conditions as may be determined.

The DPA's data protection framework, modeled after the European Union General Data Protection Regulation (EU GDPR), should adopt similar evaluation metrics in determining adequacy, thereby strengthening the Kenyan IPDT flow regime.

Evaluation metrics will allow corporate entities to determine the legality of their IPDTs to foreign jurisdictions.

INTRODUCTION

Commerce has become increasingly international and heavily predicated on the transfer of large quantities of personal data. Personal data protection in Kenya is regulated under the Data Protection Act (Act No. 24 of 2019) which mandates that personal data derived from data subjects within Kenya shall not be subject to a cross border data transfer unless the express consent of the data subject is obtained, or if there is proof of adequate data protection safeguards. A commensurate data protection framework in the recipient country is considered an adequate safeguard. However, the DPA neglects to enumerate the metrics that shall be used to determine the adequacy of the foreign recipient's framework.

This policy brief outlines 13 principles that need to be present within a foreign jurisdiction's data protection framework in order to be considered 'adequate' to the DPA and its subsequent regulations.

RESEARCH OVERVIEW

This study determined elements that may be to evaluate the proportionality of a foreign jurisdiction's data protection framework by conducting a comparative and situational analysis of the DPA and the EU GDPR and its supplemental guidelines (Article 29 Data Protection Working Party Adequacy Referential Guidelines) on cross border data transfers.

EVALUATION CRITERIA for FOREIGN DATA PROTECTION FRAMEWORKS

We propose that the following 13 principles should be present in a foreign jurisdiction's data protection framework in order to be considered 'adequate' to the DPA and its subsequent regulations:



i.
Basic concepts and data protection terminology:

The recipient country must have incorporated basic data protection concepts and terminology into their data protection framework. Examples of concepts include “personal data”, “processing of personal data”, “data controller”, “data processor”, “recipient” and “sensitive data”.

ii.
Provide Grounds for Lawful, Fair and Legitimate data processing activities:

The recipient country's data protection framework must entrench the principle that data must be processed in a lawful, fair and legitimate manner, and explicitly state the legitimate bases that may be relied upon to process the personal data.

iii.
Purpose Limitation Principle:

The recipient's data protection framework should incorporate safeguards that require personal data to be processed for a specific purpose and subsequently used only insofar as it is not incompatible with the initial purpose of the processing.

iv.
Data Accuracy and Data Minimization Principle:

Data should be accurate, adequate, relevant and not excessive in relation to the purposes for which they are processed.

v.
**Storage
Limitation
Principle:**

Data should, as a general rule, be kept for no longer than is necessary for the purposes for which the personal data is processed. The principle implies that once personal data satisfies the purpose for which it was collected, the personal data should be deleted or stored in a format that no longer identifies the data subject.

vi.
**Security and
Confidentiality
Principle:**

Data processing entities should process personal data in a manner that ensures security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, through the use of appropriate and scalable technical or organizational measures

vii.
**Transparency
Principle:**

The actualization of the transparency principle is predicated on data subjects being duly informed of all the main elements of the processing of their personal data in a clear, easily accessible, concise, transparent, and intelligible form.

viii.
**Provision of Data
Subject Rights:**

The recipient's data protection framework should provide data subjects with the right to access their personal data being processed, rectify the personal data, request for the personal data's erasure, or, under certain circumstances, object to part or whole of the processing of their personal data.

ix.
**Restrictions on
Onward Transfers
of Personal Data**

Personal data subjected to a cross border transfer should only be transferred between clearly defined parties to the transfer. The recipient's data protection framework should not permit onward transfers of the personal data to third parties not authorized to receive the personal data.

X.
Existence of penalties and sanctions promoting compliance with the data protection framework:

The recipient country's data protection framework should impose effective and dissuasive penalties for non-compliance. This is in a bid to ensure a high degree of accountability and awareness among data controllers and data processors of their legal obligations, tasks, and responsibilities.

xi.
Enshrine the principle of Accountability:

The principle of Accountability is predicated on data controllers, and/or those processing personal data on their behalf, comply with data protection obligations, and to be able to demonstrate such compliance in particular to the relevant, competent and independent data protection supervisory authority.

xii.
Provision of legal remedies for infringement of data subjects' personal data rights:

Data subjects should be able to pursue legal remedies to enforce their rights rapidly and effectively, and without prohibitive cost in the foreign jurisdiction to which their personal data is being transferred to. This includes judicial redress and compensation for losses or harm incurred as a result of a breach of their personal data.

xiii.
Monitoring and Review mechanism for Adequacy Decision:

The following procedural considerations should be incorporated in the data protection framework:

- A taskforce to monitor developments that could affect the functioning of an adequacy decision;
- Information sharing procedures with foreign data protection authorities, such as the ODPC, to facilitate periodic reviews of the adequacy decision; and
- Empower foreign data protection authorities, such as the ODPC, to review, amend, or suspend existing adequacy decisions.


CONCLUSION

The inadequate nature of the current IPDT framework under the Kenyan DPA enables organizations to flagrantly conduct cross border data transfers without concern for their data subjects and the possible violation of their privacy-related rights in foreign jurisdictions. Kenyan data subjects are not afforded the opportunity to seek redress for infringements and misuse of their personal data abroad. The adoption of the 13 principles, enumerated above, into Kenya's data protection framework will supplement the current inadequacies of cross border data transfers conducted on the basis of adequacy to the Kenyan DPA.



Strathmore University

*Centre for Intellectual Property and
Information Technology Law*



This study was made possible by a grant provided by the Hewlett Foundation.
We thank the organization for their continued support.



© 2021 by Center of Intellectual Property and Technology Law (CIPIT). This work is licensed under a Creative Commons Attribution – NonCommercial – ShareAlike 4.0 International License (CC BY NC SA 4.0). This license allows you to distribute, remix, adapt, and build upon this work for non – commercial purposes, as long as you credit CIPIT and distribute your creations under the same license:

<https://creativecommons.org/licenses/by-nc-sa/4.0>