Article by ODPC Commissioner - TRANSFER OF PERSONAL DATA ON THE BASIS OF AN ADEQUACY DECISION (Kenya) - 15th March

In the last five weeks we've established there's an increasing importance of cross-border data flows with the upsurge in globalization and e-commerce. Building trust between countries and territories, therefore, becomes important and requires an assurance that countries are like-minded in the way they approach data protection and privacy in Cross-border personal data flows.

In our ongoing series, we have covered the transfer of personal data on the basis of appropriate safeguards, necessity, and consent. In the final excerpt, we will focus on the transfer of personal data on the basis of an adequacy decision. A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory, or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.

As a result of adequacy decisions, personal data can flow freely and safely from Kenya to other countries, without being subject to any further conditions or authorizations. Adequacy does not require the other country's data protection system to be identical to the one of Kenya but involves a comprehensive assessment of a country's data protection framework, both of the protection applicable to personal data and of the available oversight and redress mechanisms. The Data Commissioner may also publish on its website a list of the countries, territories and specified sectors within that other country and relevant international organization for which the Data Commissioner has made a decision that an adequate level of protection is ensured.

A good example is the recent adoption of the European Commission's adequacy decision for the transfer of personal data from the European Union to the Republic of Korea under the General Data Protection Regulation.

Cross-border data transfers allow businesses and consumers access to the best available technology and services, around the world which is important to the growth and success of the global economy. Ensuring data protection and privacy in cross-border data flows does not stifle international trade but rather enables it.

Article by ODPC Commissioner TRANSFER OF PERSONAL DATA ON THE BASIS OF CONSENT - (Kenya) 8th March

The unprecedented growth in e-commerce has revolutionized the way we make purchases online, providing wider choices, payment, and delivery options. In the fourth excerpt of our ongoing series, we'll focus on the transfer of personal data on the basis of consent.

Consent is one legal basis for processing information. A data controller or processor must seek consent from a data subject for the transfer of sensitive personal data outside of Kenya. Additionally, in the absence of an adequacy decision, appropriate safeguards, or prerequisites for transfer as a necessity, a transfer of personal data to another country should take place only on the condition that the data subject—

(a) has explicitly consented to the proposed transfer. Data controllers and processors have a responsibility to give people genuine choice and control over how they process, use, and store their data. They should ensure that the data subject has the capacity to give consent, gives it voluntarily, and that the consent is specific to the purpose of processing.

For example, a Kenyan bank collects its customer' data for the specific purpose of loan application without considering transferring this data, to a third party outside the country. However, some years later, the same bank is acquired by a South African bank that wishes to transfer the personal data of its customers to another bank outside Kenya. For this transfer to be valid on the basis of consent, the customers should give their consent for this specific transfer at the time when the transfer is envisaged.

(b) Data subjects are to be informed of the specific risks resulting from their data being transferred to a country that does not provide adequate protection. The provision of this information is essential to enable the data subject to consent with full knowledge of these potential risks.

This information should ideally be provided in a data protection policy notice which must be simple, clear and provided in a language that the data subject can understand. The notice should, for example, include information that there might not be a data protection authority or data protection legislation to govern the processing of personal data in the third country.

It is the responsibility of the data controller or processor to bear the burden of proof for establishing a data subject's consent in the cross-border transfer of their personal data.