Data Sharing and Cross border data transfer – options and solutions

DATA PROTECTION CONFERENCE

JANUARY 2016

HANNAH AGBOZO

Cross – Border Transfer is happening

* Data sharing with non-resident affiliates
* Data sharing with independent service providers
* Shared Services/ Outsourcing
* Business Process Outsourcing Transactions (BPOs)

Current Legal Framework

* No general provision covering the export of data

* Section 18 (2) of the Data Protection Act, 2012 (Act 843)

Controller or processor shall ensure that data in respect of ***foreign data subjects*** is processed in compliance with data protection legislation of the foreign jurisdiction of that subject.

* Section 30 (4) ***Data controllers*** shall ensure that a foreign data processor complies with "*the relevant laws of this country*".

* Note: Duty of due diligence placed on data controller
* S 30 (4) relates to compliance with "*security measures.*"
* Interpretation Issues?

Regional Guidance ?

* Article 19 (I) of the ***ECOWAS Supplementary Act on Personal Data Protection*** (A/SA.101/10) (Feb 2010)
* DPA's to authorize the transborder transfer of personal data
* Article 10 (6)k of the ***African Union Convention On Cyber Security And Personal Data Protection*** requests for opinion, declarations and applications for authorization shall Indicate envisaged transfer of personal data to a third country that is not a member of the African Union, ***subject to reciprocity***".

Regional Guidance?

* 14 countries surveyed in Western, Central Africa & East Africa
* Response to the question: *Does your law or licence specify where servers, containing customer data should be located? For example does the law or licence specify if the customer data records should be stored in country or outside the country. Is there a prohibition against having such servers outside the country?*
* All 14 countries had no express provision in their Data Protection or Similar statutes on the matter of export or transfer of personal data
* In 4 of the countries some regulator or governmental agency had issued directives either banning it outright or asking that it be done with its consent or approval.

The EU example - Options

* **EU Model Controller Contract :**
* **Safe Harbor Certification:** Self- regulatory privacy framework that required self-certification with the US Department of Commerce that a company adheres to the 7 Safe Harbor Privacy Principles (*Notice, consent, onward transfer, access, data security, data integrity and enforcement*). * CJEU ruled on October 6, 2015 that Safe Harbor Certification was invalid with immediate effect.
* **Binding Corporate Rules**
* **Consent**
* **ICC Clauses**
* **Certification of Adequacy**

Charting a Way Forward

* Guidelines for export and import of data? (create certainty for business, risk assessment and clarity with compliance)
* Measures adopted should be simple, inexpensive and developed with flexibility in mind – ICT savvy

Consider:

* Certification of Adequacy of Data Protection laws of certain countries. For eg. countries belonging to the EEA. Require Notification of transfer with details of Data Processor
* Reciprocal arrangements
* Standard clauses or Model Contracts -
* Corporate Guidelines
* Self Certification
* Consent of data subject/necessity of export to fulfil purpose of collection or perform contract

THANK YOU!