COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 4. March 07, 2019
Data protection adaptation in emerging economies a 'Herculean task' - A conversation with Ibrahim Yeku

About Ibrahim

Ibrahim Yeku is a Barrister at Solola & Akpana in Port Harcourt, Nigeria. His work focuses on intellectual property, corporate compliance and insolvency, information technology and electronic commerce, maritime law, and international trade and WTO agreements.

***RSCC*: What are some risks that are particular to emerging economies?**

IY: When you talk of peculiarity of risk in emerging economies, you talk of the peculiarity of opportunities in the emerging economies as well. Some of the particular risks in emerging economies include political risk, data risk, corruption risk, and compliance and regulatory risk. The incentives to doing business in emerging economies are high because of the cheap labor, access to raw materials and large population. Inherent in the opportunities in emerging economies are risks that cannot be ignored. Any organization that ignores these risks will be doing so to its detriment. The way to maximize opportunities in emerging economies is to set up appropriate mitigation measures that will help de-risk the risks and convert the risks to profits.

***RSCC*: Data privacy and protection has been referred to as a "first world" problem. What do you think of this statement?**

IY: As a matter of culture, the concept of privacy is alien to the lifestyle of the people in emerging economies of Africa and Asia. In these emerging economies, there is a strong sense of communal bond and communal accountability, which gives little or no room for the right to be left alone. This lifestyle also affects the disposition of other actors in the society, including the government. Until recently, most countries in emerging economies did not have specific legislation on data protection, aside from what is provided in the national constitutions as a fundamental right. The coverage of privacy rights under national constitutions does not really address modern day data protection challenges.

Furthermore, the slow pace of technological penetration in some of the emerging economies made the issue of data of no concern before now. The first world cares so much about privacy, because certain aspects of first world culture emphasize the right to privacy. More so, the advancement in technology and technology infrastructure in the first world makes data privacy and breaches of privacy a major source of concern; however, with the advent of the internet and globalization, privacy risk is now a global risk of mutual concern to both the first world and emerging economies. The world is shrinking, so also is the private space of individuals. Learning to be safe in an intrusive world is a Herculean task.

***RSCC*: When you address mitigating factors and strategies for preventing breaches in emerging economies, who is your target audience? Do companies originating out of emerging economies devote time and effort to data privacy and protection?**

IY: The target audiences are companies operating within the emerging economies and originating out of the emerging economies. No doubt, transnational companies operating within the emerging economies appreciate

the importance of data privacy despite the fact that there is no local legislation or it is insufficient on the subject. The awareness of the transnational companies flows from legislation in their parent countries, which impose obligations with respect to the rights of data subjects beyond territorial boundaries. So, the challenge for transnational companies is mainly how to maintain high privacy standards in countries without privacy safety standards.

A European company operating in Togo will not ignore the obligations imposed on it under the GDPR because of the inadequacy of data protection regimes in the country; however, companies originating from the emerging economies have yet to appreciate the full scale of responsibility of data protection. A majority of these companies have yet to align their operations to satisfy the requirements of local data protection legislations. This is partly because the regulatory bodies are weak or not alive to the responsibility of ensuring compliance. Regarding the GDPR, it is viewed by these companies as a "busy body" legislation, which cannot be enforced against them in the event of a violation or a breach of data that relates to European citizens. Running an effective data protection program requires some level of resources, which companies originating from emerging economies are unable to expend.

***RSCC*: There are some data protection regulations coming out of emerging economies, such as South Africa's privacy law. How do they compare or contrast with GDPR and U.K. and U.S. data protection frameworks?**

IY: The National Information Technology Development Agency [of Nigeria] has taken the initiative to issue data protection regulation in Nigeria. This is the first regulation in the absence of substantive law on this subject that addresses the concern of data breaches and privacy rights. This initiative came about in due to the leadership of Dr. Isa Ali Ibrahim Pantami, the Director General of the agency.

In South African law, the right to privacy is protected by the common law and Section 14 of The Constitution of the Republic of South Africa, 1996. The Protection of Personal Information Act (2013) recognizes the right to privacy enshrined in the Constitution and gives effect to this right through mandatory procedures and mechanisms for the handling and processing of personal information.

In Africa, 18 countries (Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Mali, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Malawi, Morocco, Niger, Senegal, South Africa, Tunisia and Zambia) have enacted data protection and privacy laws. Six countries have laws in draft stages (Kenya, Nigeria [substantive law], Togo, Tanzania, Uganda and Zimbabwe). The remaining countries either have no legislation or have no data available.

The U.S. does not have a comprehensive data protection law that covers all sectors; however, there are sector-based privacy legislations that govern different aspects of personal privacy. The Data Protection Act 2018 is the U.K.'s implementation of the General Data Protection Regulation.

Across North America and Latin America, 17 countries (Canada, U.S., Mexico, Nicaragua, Jamaica, Trinidad and Tobago, Nicaragua, Costa Rica, Colombia, Peru, Bolivia, Chile, Argentina, Paraguay, Uruguay, Bahamas and Dominican Republic) have legislation. Four countries are drafting legislation (Ecuador, Honduras, Panama and Brazil), while the others either have no legislation or no data available to determine whether a law was in place.

***RSCC*: Is the GDPR and the general trend toward more regulation of data sweeping into emerging economies, as well? If so, what drives it? Is it different from what we're seeing in developed economies?**

IY: Yes, most companies in emerging economies with a vested interest in the EU are adopting the GDPR framework for the development and management of privacy programs. The extraterritorial jurisdiction of the GDPR is a major causative factor for companies to be mindful of its provisions in emerging economies. The GDPR is a model template for data protection in the world. Most countries are adopting the provisions and designing

their privacy legislations to be in line with the GDPR. There is a high level of "privacy right consciousness" in the developed world. Companies could be fined huge sums of money as a result of a breach of data. The fear of fines or sanctions is another driver of compliance with the data protection law in the developed world.