Compliance & Ethics Professional

February
2015

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Compliance and Ethics at Abt Associates

an interview with Bonnie Bass and Jeanine Hubler

Senior Subcontracts Manager

Senior Director, Finance, Administration and Operations

See page **14**

by Jan Dhont and Katherine Woodcock

Data localization requirements: Growing trends and impact for company compliance

» Recent development and proliferation of data localization laws have been furthered by the NSA spying revelations.

» Localization laws require businesses to take measures to ensure various forms of data are stored within national or regional borders.

» Russia, South Korea, Brazil, Vietnam, and Indonesia already have localization laws in place, amongst others.

» The changes will have huge potential impact on companies, because current data flows, storage, and IT infrastructure and solutions will have to be rethought

» We could see development of local and regional IT and cloud services; however, this will come at a cost to companies and businesses.

Catalyzed by the Snowden revelations, many governments are now pushing forward new data localization laws. These laws, in theory, aim to ensure the privacy and security of their citizens and enable domestic growth within the technology sector. This article explains the background and recent trends behind data localization, turning to the practical consequences for companies and businesses.

Dhont

Woodcock

What is data localization?

Data localization laws set forth requirements to keep and store data "locally" (i.e., within national or regional borders). Countries that adopt such laws require the storage or processing of data on servers physically located within their borders. In broad terms, data localization obligations may also be laws that hinder or restrict the transfer of data across national borders.

The type of data targeted can be sector-specific, such as financial data that is being considered by the South Korean Financial Services Commission, or based on the nationality of the individual, the so-called "data subject" to whom the data relates. Other laws are more all-encompassing, such as all data held by internet service providers (ISPs) and telecommunications and mobile network providers within a certain border. Many critics equate stringent rules regulating the use of personal data, such as data protection and security laws—like those in place in the European Union (EU)—as acting in effect as data localization laws. This criticism derives from the argument that restrictions on data transfers from certain borders create high regulatory hurdles for companies to comply with—in effect, requiring the

increasing localization of data storage within those borders.

Where are these rules popping up?

Data localization laws have been passed in South Korea, Russia, Indonesia, Vietnam, and Brazil, amongst other jurisdictions. Other countries, such as India, are also contemplating data localization requirements, but some others are still looking to expand existing regulations, including South Korea and Indonesia. As mentioned, many sources indicate that the comprehensive privacy and data protection reforms within the EU will also further expand the rules in place there, via the proposed draft General Data Protection Regulation that is currently under negotiation within the legislative process. Below we will briefly look at a few of these data localization laws.

Data localization laws have been passed in South Korea, Russia, Indonesia, Vietnam, and Brazil, amongst other jurisdictions.

Brazil

Brazil's Federal Senate approved the Marco Civil da Internet in April 2014. Originally drafted to protect Internet user rights, following the NSA spying revelations additional provisions were added. A controversial piece can permit the Brazilian government to require "connection providers" and ISPs to use or install technology or data center infrastructure in Brazil. Worryingly, violators are subject to penalties of up to 10% of their Brazilian gross proceeds.

Russia

In 2013, the Russian Ministry of Communications drafted an order that requires telecommunication providers and ISPs to ensure that data can be collected and maintained for at least 12 hours. Expanding on these initial efforts, in July 2014, Federal Law no. 242-FZ was passed, requiring the storage and processing of personal data of Russian citizens in databases within the Russian territory. This law also requires the disclosure of the location of these data centers to the Russian authorities. Although these changes may trigger mere duplication of data within Russia, its application casts a wide net – triggering affects not only for Russian companies or companies with a Russian legal presence, but also multinationals with Russian customers, employees, or contacts, including retail companies that target the Russian market.

Vietnam & Indonesia

In September 2013, Vietnam's Decree on Management, Provision and Use of Internet Service and Information Content online became effective. Requiring ISPs to maintain copies of information to allow inspection by the Vietnamese authorities seems, at first glance, not overly rigorous. However, companies are specifically required to have a server or data system within Vietnam to permit the inspection and to be able to hand over the information to the relevant authorities. These rules have a broad application to websites, social media outlets, mobile networks, and gaming providers reaching out to the Vietnamese market.

Similarly, Indonesia's 2012 Regulation 82 on the Operation of Electronic System and Transaction Operation requires companies to have data centers and disaster recovery centers

in the territory of Indonesia. The Ministry of Communication recently published a draft regulation contemplating an expansion of this requirement, so that all organizations providing services in Indonesia should have domestic disaster recovery systems.

Which companies will be the most significantly impacted?

Alarmingly, localization laws can potentially affect any business that uses the Internet or web-based technologies for services. These laws affect ISPs, social media, and mobile communications companies generally. But they will also hit multinationals and small and medium-sized enterprises (SMEs) active in retail, production, healthcare, pharma, and other business sectors. This stems from direct application of these laws to global technology services as well as web-based technology. These laws will have residual effects for all industries and organizations that use such services and are active in the relevant jurisdictions. Potentially, these laws can affect everyone from multinational companies to local farmers to the extent they rely on web-based technology or services, for example, for payroll or for transactions.

What does this mean for companies?

Companies that fall within the scope of data localization laws will need to invest in building local infrastructure to comply with these regulations. Businesses will have to carefully decide whether to enter or continue to be active in these increasingly restricted markets. Alternatively, they can also step away from reliance on more advanced technology solutions; however, in practice, this strikes at competitiveness and cost saving, leaving little choice for smaller players without access to bigger resources.

Organizations will need to increase investment in the construction and maintenance of their own local IT infrastructure and, correspondingly, data security mechanisms to ensure the information is adequately protected. One effect is that companies may no longer be able to utilize cheaper computing solutions such as cloud-based technology. It is predicted that countries and regions will now have their own servers and data centers for Internet services as well as for data collection, storage, and access.

Organizations will need to increase investment in the construction and maintenance of their own local IT infrastructure and, correspondingly, data security mechanisms to ensure the information is adequately protected.

Finally, companies will also need to put increasing focus on data segregation by the nationality of the individual to whom the data relates. Many recent technological advances, such as big data analytics, may be affected or accessible when subject to data localization; aggregation of truly global data sets would be severely impeded if not prevented all together. ✳

Jan Dhont *(j.dhont@lorenz-law.com) is a Partner and* ***Katherine Woodcock*** *(k.woodcock@lorenz-law.com) is Senior Associate, both at Lorenz in Brussels, Belgium.*