In recent years, Asia has seen a push by governments to implement data localization laws. Such laws require businesses to ensure various forms of data are processed and stored in servers physically located within national borders.

A number of countries in the region — including China, India, Indonesia, South Korea, and Malaysia — have already introduced data localization requirements, and there are efforts across Asia to introduce or enhance such regulation. The arguments for such regulations range from enhancing national security, protecting personal privacy, aiding law enforcement, and preventing foreign surveillance, in addition to appeals to the principle of sovereignty. But governments have also restricted the transfer of data across national borders in order to foster the development of domestic technology sectors. Furthermore, governments have implemented data localization policies as a short-term means of promoting economic development via the construction of in-country data centers and the creation of highly-skilled technical jobs.

On the other hand, a number of markets in the region have not joined the trend, including Myanmar, Cambodia, Philippines, Hong Kong, Singapore, Thailand and Japan. Singapore stands out for its differentiated approach. Instead of pursuing localization, it is focusing efforts on promoting its digital economy, harnessing data analytics, and creating the best possible ecosystem for digital technologies to thrive across all sectors.

Data localization policies can have real downside impacts on foreign investors: they complicate the management of international technology infrastructure, limit a company’s ability to transfer data from place to place, and add operation costs as businesses are suddenly mandated to build expensive local data centers.

Recognizing the risks and looming compliance costs, multinational firms advocated strongly for regional trade agreements that would ease the trend of data localization and allow data to flow more freely across borders. The centerpiece of this push was the Trans-Pacific Partnership (TPP), which included specific provisions meant to limit data localization (which the agreement called “digital protectionism”), prohibit digital customs duties, and enable cross-border data flows.
Singapore stands out for its differentiated approach. Instead of pursuing localization, it is focusing efforts on promoting its digital economy, harnessing data analytics, and creating the best possible ecosystem for digital technologies to thrive across all sectors.

But TPP was dealt a significant blow in January when new US President Donald Trump withdrew the US from the agreement. Some participating governments are now considering moving forward without the US, but ratification in any form now looks much less likely. In its place, Asian governments are now doubling down on negotiations for a China-led Regional Cooperative Economic Partnership (RCEP) agreement. But while the RCEP would be a positive step forward on trade liberalization, it is shaping up as a much less ambitious agreement. The final RCEP text is still under negotiation, but with China in a leading role, and with Beijing an advocate of localization policies, it is very unlikely that the agreement will go nearly as far as TPP in addressing the issue.

So Asian governments will continue to pursue disparate data localization policies for the foreseeable future. This means the fragmentation of data flows and storage across the region, which will raise operational costs to business and reduce efficiencies in the e-commerce sector.

Our in-country FTI analysts across Asia are seeing this trend play out, as countries in the region are now aggressively moving forward with new standards for the management of data. A good example of the trend toward data localization is Indonesia, where the government is pushing an agenda of technology innovation, in particular in the FinTech and e-commerce sectors. Indonesia’s draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet would broadly require that internet audio, video or other media (over-the-top, or OTT) service providers place part of their data centers within Indonesia. Additionally, the draft Indonesian Regulation on Technical Guidelines on Data Centers would mandate any institutions that provide information technology-based services to build local disaster recovery data centers.

Similar to Indonesia, Vietnam’s draft OTT Circular would require all OTT service providers to locate at least one server in Vietnam. China’s recent draft Supervision Rules on Insurance Institutions Adopting Digitized Operations would also require localization of data servers by any insurance institution processing the personal data of Chinese citizens. In South Korea, a draft Standards for Cloud Computing Services would require all cloud computing providers to have public data centers located within the country.

Real costs to business
These laws pose an increasing threat to Smart Nation initiatives by fostering unfavorable conditions for digital economies to thrive, while also creating the potential for companies to withdraw from key markets, further fragmenting the global Internet and restructuring information technology infrastructures.

They can also have substantial negative ramifications for local economies. In 2014, the European Centre For International Political Economy calculated that the impact of recently proposed or enacted legislation on GDP and overall domestic investments in a number of Asian countries. The calculated impact on GDP in China is -1.1%; India -0.1%; Indonesia -0.5%; Korea -0.4%, and Vietnam -1.7%, while the impact on domestic investments was: China -1.8%; India -1.4%; Indonesia -2.3%; Korea -0.5%; Vietnam -3.1%.

Companies in Asia must remain aware of and engaged on incoming data localization laws and the potential impact to their business and associated costs. FTI Consulting Strategic Communications’ professionals across the region track issues, advocate positions and engage with regulators and stakeholders to help companies prepare for and navigate incoming regulation.

Examples of current country-by-country data localization legislation

China

- China’s Online Publishing Service Management Rules requires that all servers used for online publishing in China be located within the borders of the PRC.
- The Administrative Regulation on the Credit Information Industry and Credit Reference Agencies requires all credit information collected on Chinese citizens to be processed and stored within China and does not allow the transfer of that data outside of China’s borders.
- The Population and Healthcare Information Management Measures prohibits the overseas transfer of health and medical information.
- The Cyber Security Law of China will come into force 1 June 2017 and requires that “important data” of citizens, collected or produced by key information infrastructure operators during their in-country operations, should remain within China.

So Asian governments will continue to pursue disparate data localization policies for the foreseeable future. This means the fragmentation of data flows and storage across the region, which will raise operational costs to business and reduce efficiencies in the e-commerce sector.
India

- India’s National Data Sharing and Accessibility Policy requires all data collected using public funds to be stored within the borders of India.

- In 2014, the National Security Council proposed (1) that email service providers must host servers in India, (2) data generated from within India must be hosted in India, and (3) that mirroring of data to servers abroad is prohibited.

- The National Security Advisor also asked the Department of Telecom to look at the possibility of making it mandatory for all telecom and Internet companies to route local data through the National Internet Exchange of India.

Indonesia

- Indonesia’s Regulation No. 82: Information and Electronic Transaction Law mandates companies that provide internet services directly to the consumer must locate their data centers within Indonesia.

South Korea

- South Korea’s Land Survey Act bans the provision of online mapping services via foreign servers.

Malaysia

- Malaysia’s Personal Data Protection Act requires data about Malaysians to be stored on local servers.

Vietnam

- Vietnam’s Decree of Information Technology Services mandates that all companies providing internet services maintain at least one server within the borders of Vietnam.