EU ASIA
Financial Services Round Table

# POSITION PAPER

## EUAFSRT RECOMMENDATIONS ON DATA LOCALISATION REQUIREMENTS IN ASIA-PACIFIC

## FEBRUARY 2019

**Overview of market concerns**

We welcome the European Commission's recent response to the consultation by the Indian Ministry of Electronics and Information Technology (MEITy) regarding concerns related to the draft Personal Data Protection Bill. We agree that India and Europe share important values regarding protecting data privacy and that while the MEITy Data Protection Bill is an important step, the requirements for localisation are a serious concern for European businesses active in India. It is worth noting that European businesses have raised similar concerns regarding data localization requirements across the APAC region, as several jurisdictions have already implemented or plan to implement comparable requirements.

We urge the European Commission to continue to engage with governments across APAC highlighting its concerns regarding data localization and its importance to international business and risk management, but also for the purposes of information sharing to tackle cyber and financial crime. We see a number of opportunities to raise these issues in both the bilateral and multilateral engagements with governments across APAC during 2019. Relevant forums for engagement include the EU-Asia Financial Services Forum on Financial regulation, the EU-China High-level Economic and Trade Dialogue and the ASEAN-European Union Dialogue. As the EU continues its efforts to negotiate trade agreements and facilitate the operation of EU companies offering services in APAC through other bilateral and multilateral agreements and negotiation, it should actively seek to warn about the risks of data localization requirements.

**The risks of data localisation**

Several countries across the APAC region have implemented or are in the process of drafting regulations or legislation that mandate some kind of data localisation[1]. Data localisation requirements are usually put in place for reasons including national security, domestic economic concerns, protecting citizens' privacy and maintaining national sovereignty. These requirements are typically found in data privacy laws (e.g. India) or cyber security laws (e.g. China), though some jurisdictions have government bodies that have acted independently to introduce data localisation requirements in areas they see as high risk (e.g. Australia's health laws). These laws may have explicit data localization requirements, but other regulation, specifically that for financial services, often contains *de facto* data localization requirements.

[1] Includes China, India, Australia, Malaysia, Brunei, Indonesia, Vietnam, and the Philippines.

This trend represents a significant challenge to European companies that sell goods and services in the region as it increases the cost of compliance, restricts companies' ability to utilize new technologies such as data analytics, cloud and artificial intelligence, restricts data transfers, complicates commercial exchanges; increases the cost of compliance and creates an uneven playing field that benefits locally established companies over European ones. Further, by fragmenting the location of data, the requirements also make it more difficult for firms to effectively secure that data. Arguably, if the policy aim is to protect the personal data of citizens, then requirements to onshore data ultimately do not achieve that objective.

The fragmentation of data flows in APAC have a significant negative effect on the efforts dedicated to law enforcement to fight financial crime, as it limits the ability of financial institutions and corporates to share information that could lead to valuable insights on money laundering and fraud risks and the mitigation of potential financial crime threats.

Data localisation is also believed to have direct economic repercussions. The Information Technology & Innovation Foundation released a report in 2017 that estimated that the costs to national GDP of data flow barriers (including localisation) could "reduce U.S. GDP by 0.1-0.36 percent; cause prices for some cloud services in Brazil and the European Union to increase 10.5 to 54 percent; and reduce GDP by 0.7 to 1.7 percent in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam".[2]

As governments look to modernize their data privacy frameworks, they should aim to do so in a way that protects citizens' data while allowing for the free flow of data that facilitates commercial and economic growth. While we would encourage the European Commission to highlight Europe's values regarding data privacy and protection there are major markets in the region that offer examples of jurisdictions with modern privacy frameworks that do not have data localisation requirements including Hong Kong, Singapore, and Japan. While there are differences between their respective privacy regimes these jurisdictions offer a model that other Asian countries could also look to as an example.

**Recommendations**

Taking into account the issues outlined above we urge the European Commission to consider the following recommendations:

1) Utilize existing bilateral and multilateral forums to proactively advocate for the free flow of data to avoid restrictions to trade in services created by data localisation requirements. This includes the ongoing free trade negotiations with India, ASEAN as well as bilateral negotiations with

[2] Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," Information Technology & Innovation Foundation, May 2017, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-arebarriers-and-what-do-they-cost

countries in the region; the EU-Asia Financial Services Forum on Financial regulation, the EU-China High-level Economic and Trade Dialogue and the ASEAN-European Union Dialogue.

2) In those forums we would encourage the European Commission to
    a. Emphasize the importance that a modern personal data protection regime has in facilitating economic growth and the importance that a formal framework has in ensuring businesses are able to work within a stable legal framework.
    b. Make clear the negative effects of data localization on the harmonization of a business' technology estate and the concurrent negative impacts on cybersecurity and operational resilience that this brings.
    c. Highlight the risks that data localisation requirements poses to the effective use of data by law enforcement to prevent financial crime.
    d. Highlight the importance of the free flow of data in the development of innovative technologies, SMEs and economic growth.
    e. In the context of FTAs, request chapters on data flows that set out commitments to ensure the free flow of data and prevent the implementation data localisation requirements.
    f. Encourage governments in APAC to follow Europe's example with regards to legitimate interest exemptions to ensure clarity for the financial sector when conducting customer due diligence.
    g. Pursue bi-lateral agreements with key jurisdictions in APAC that ensure the ability of firms to move data between the two parties.

***

*The EU-Asia Financial Services Roundtable promotes a shared understanding of the regulatory issues faced by financial markets participants in Europe and Asia, while also shaping the EU-Asian regulatory and policy discussions. Its members are Afore Consulting, AIG, DTCC, HSBC, IHS Markit, London Stock Exchange, Moneygram, Moody's, Nex, Refinitiv, Standard Chartered.*

*It supports regulators in developing an appropriate and balanced regulatory framework that enables long-term growth in both Europe and Asia, whilst identifying areas where regulation impedes the international flow of capital or creates unnecessary barriers to doing business. It supports the development of regulatory best practice, and a level playing field in financial services regulation in Europe and Asia, whilst promoting open and stable financial markets.*