HERBERT SMITH FREEHILLS

INCREASING LOCALISATION OF DATA IN ASIA: WHY THIS MATTERS FOR TECH

09 December 2021 | Asia

We are seeing a trend towards data localisation emerging in certain countries in Asia which is raising business-critical issues for the tech sector. Usually thought of as just a data privacy tool, regulation restricting cross-border transfers of data are gaining support with legislators in China, India, Vietnam and Indonesia as a way to protect national sovereignty and security.

WHAT IS DATA LOCALISATION?

Data localisation or data residency laws require companies to store data locally (i.e. inside the country of collection). In some cases, the laws extend to processing data locally and mandate individual or government consent for out-of-country transfers. Such requirements are driven by national security or public interest. Depending on the jurisdiction, the data in question can be:

- important data (e.g. important data handled by critical information infrastructure operators ("**CIIO**") in China); and
- personal data (e.g. personal data handled by CIIOs or organisations handling a large amount of personal data in China, personal data under the cybersecurity law and the draft decree on personal data in Vietnam, and critical personal data and sensitive personal data under the draft privacy bill in India) .

In Indonesia, public electronic systems operators' data centres must be located onshore.

Data localisation laws in this article refer to the requirement to store data onshore, which is an additional requirement to the usual cross-border data transfer restrictions under data privacy laws.

WHY THIS MATTERS

Data localisation laws affect both sides of the digital economy equation (i.e. customers and suppliers). Even if your business isn't directly affected, the business of your customers may be. This can have ripple effects both up and down the supply chain.

IN THE REGULATORY LANDSCAPE ACROSS ASIA

There is no harmony at a regional level when it comes to data localisation regulation in the Asian region. This means navigating the regulatory landscape can be tricky, especially when regulated sectors (such as telecoms, banking and insurance) are involved.

Data localisation laws take different forms in Asia. Such requirements may apply to sensitive or critical personal data and are embedded under the privacy laws (e.g. the draft data privacy bill in India), or in the case of China, such requirements apply to both important data and personal data and are set out across the Cybersecurity Law, Data Security Law and the Personal Information Protection Law. In Vietnam, data localisation requirements are set out in its Cybersecurity Law and draft decree on data protection (i.e. Vietnam's draft privacy law). In Indonesia, the data localisation requirement is applicable to public electronic systems operators only.

QUESTIONS TO ASK IF YOU'RE A TECHNOLOGY COMPANY

At the outset, technology companies should be asking themselves: *are our products, services or business activities (or those of our customers) caught by data localisation laws?*

Regional expansion plans can be quickly scuppered if businesses do not have a comprehensive understanding of the data localisation laws in the countries they are targeting. For example:

MONUMENT ICONS-01.PNG	**VIETNAM** Under its Cybersecurity laws and decrees, foreign providers of online services (such as e-commerce, online content, payment, social network and social communication) may be required to store data in Vietnam and set up a local branch or representative office. The situation is different in Indonesia where "*public electronic systems operators*" that provide public services must establish a local data centre.
MONUMENT ICONS-02.PNG	**CHINA** Personal information held by CIIOs must be stored in China and can only be transferred out if official security assessment approval has been obtained. Most private businesses are not likely to be CIIOs but their customers can be (e.g. State Owned Entities), which may require their vendors to help them comply with data localisation laws. Separately, data processors handling a large amount of personal information must also store personal information in China per the Personal Information Protection Law.

The other question technology companies should be asking themselves is: *is the data we collect regulated under data localisation laws?*

MONUMENT ICONS-02.PNG	**CHINA** The Cybersecurity Law and Data Security Laws regulate the storage and transfer of "*important data*". Important data held by CIIOs in China must be stored in China and can only be transferred outside of China if security assessments have been passed. Although this data category is not yet clearly defined, important data, by definition, includes data which, if compromised, may have a significant impact on national security, the public interest and economic development of the country.
MONUMENT ICONS-03.PNG	**INDIA** The proposed Privacy Bill requires a data transferor in India to retain a copy of sensitive personal data in India. The Indian data privacy bill has also introduced a new concept of "*critical data*", which has not been defined. Critical personal data must be processed only in India. The Privacy Bill gives the Indian Government broad discretion to define "*critical personal data*".

RISKS OF HAVING NO DATA LOCALISATION STRATEGY

Where data localisation laws apply, you need a data localisation strategy. The increasing patchwork of data localisation laws across Asia are causing headaches for businesses (so much so that specialist 'data residency as a service' companies have emerged, offering solutions to enable regulated businesses to stay compliant). Data migration is often a costly and time-consuming process which require detailed planning. Given that most international businesses store their data across the Asian region in a centralised location, the question is whether and when data migration should be implemented for Asian jurisdictions with data localisation laws.

Having no existing data localisation strategy could have commercial implications. A key risk is that existing enterprise-wide arrangements for data storage and hosting may not be able to be leveraged if existing service providers are unable to provide in-country storage arrangements. It may also lead to difficulties synthesising data storage arrangements at a regional scale.

Further, the failure to properly plan an expansion can, at the end of the day, have significant time and cost implications for businesses, including the following risks:

1. Entry to new markets can be delayed because of the need to establish in-country storage/hosting arrangements;

2. Navigating local requirements requires local expertise and on-going regulatory monitoring;

3. Regulatory delay can have implications for products; and

4. There may be functionality impacts on applications or services in order to meet local requirements which can be a barrier to scaling quickly.

Finally, businesses need to be aware of the possible corporate structuring implications as part of setting up a data localisation strategy. For example, in the process of data migration, companies may need to set up a local entity or branch if required by the specific country's data localisation laws or make further investments in the local jurisdiction. When significant investments are made in your local entity in Asia, it is important to consider questions such as:

1. How to structure your investments in the local entity to ensure that they will be protected by international investment treaties;

2. How to protect your legitimate expectations as to regulatory stability and investments made in reliance of promises made by regulators; and

3. How to invest in compliance with data localisation laws and to protect your recourse to potential investor-state dispute settlement in the future.

Some data localisation laws and new regulations may even affect existing investments and rights, lead to losses and give rise to potential disputes with business partners and customers. As of December 2020, 71 tech companies had brought cases against states often due to changing regulations, as we observed here.

WHAT SHOULD YOU DO TO MANAGE DATA LOCALISATION RISKS FOR YOUR COMPANY?

CONDUCT A DATA MAPPING EXERCISE

Ask:

- What types of data do you currently collect and store, any important data, critical personal data or sensitive personal data?

- What countries does this data come from and where will this data be transferred to or shared?

- Where is that data currently stored? Where are the copies stored?

- Which jurisdiction's laws apply to your data?

- Do data localisation laws apply to you?

- Are your investments in data storage and processing protected by international investment protection treaties?

SET UP A DATA LOCALISATION STRATEGY

Ask:

- What types of data will be collected? From which countries?
- How will the data be stored?
- Do you need to make preparations to comply with data localisation laws as a result?
- Do you need to incorporate a local entity? How should your shareholdings be structured?
- What types of investments in the local entity and rights to data are protected investments in these countries?

We can help you navigate these considerations to help protect against the risks.

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

PEGGY CHOW
OF COUNSEL, SINGAPORE
+65 6868 8054
Peggy.Chow@hsf.com

CHRISTINE SIM
SENIOR ASSOCIATE, SINGAPORE
+65 68688064
christine.sim@hsf.com

CLARE HUBERT
SENIOR ASSOCIATE, SINGAPORE
+65 68688097
Clare.Hubert@hsf.com

LEGAL NOTICE