

GPS Technology Quarterly

What Data Localization Means for Businesses

October 2018

China's Cyber Security Law (CSL), effective on 1 June 2017, introduced a new regulatory framework for how organizations store, manage, and transfer information in the People's Republic of China (PRC). One element of the CSL – data localization – has been singled out by foreign governments and companies who are concerned that China's stricter data storage regulations will significantly impact operations.

Determining if, how, and when to localize data to China must be a risk-based, rather than a check-the-box activity. The ambiguity of the guidelines, the multiple regulators involved with differing motivations and capacities to enforce, means that certain types of data will be more prioritized than others. Companies must first have this understanding before determining the necessity and 'how to' of localization.

What is data localization?

According to Article 37 of the CSL: "Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within Mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall conduct a security assessment."

Essentially, the data localization provision requires "critical information infrastructure (CII) operators" to store certain types of data within China. Subsequent draft regulations on cross-border data transfers indicate that all "network operators" – which is any organization with three or more computers (so essentially all businesses) – must submit themselves to the security assessment before transferring this data abroad.



While CII operators are legally required to localize data, the draft cross-border transfer regulations indicate that it is very probable that network operators (as well as CII) will not be allowed to transfer “important data” outside of China. However, “personal information” is likely to be approved for transfer if strict security controls are in place.

What’s the problem with data localization?

Currently, the definitions of data and who qualifies as CII operators are ambiguous. These definitions (possibly by intention) give regulators expansive flexibility for implementation. Many multinational companies (MNCs), who built their technology operations on the premise of globalization (for instance, with servers in Switzerland and IT staff in India) are concerned that the costs of data localization requirements could run into millions.

Then why is China requiring it?

The CSL dovetails with emerging laws and rules on data storage that are being implemented worldwide. As the amount of information exponentially grows, regulators around the globe are looking for ways to manage the risks associated with privacy rights, data breaches, disinformation, criminal hackers and hacktivists.

China’s CSL – while certainly concerned with all the above – is primarily driven by national security concerns, the data localization requirement in particular. China’s cyber space regulators, the Cyberspace Administration of China (CAC), consider data to be a key national resource standpoint that is “more valuable than gold or oil.” Businesses are perceived as having too much control over that strategic resource, and so they need to be monitored, controlled and even reined in. Data localization, in the eyes of Chinese regulators, is a key component of providing authorities with that needed level of control.

What is the timeline for localization?

CII operators were legally required to localize as of 1 June 2017, when the CSL was implemented. The cross-border data transfer regulations, which apply to all network operators, have been in draft form for over one year. Regulators involved in their development have long claimed imminent finalization. Speculation over their delay generally focus on internal bureaucratic tussles over the final scope and details for data localization, and concern over releasing controversial rules during the ongoing US-



China trade war has now emerged. However, despite the delays, multiple regulators have indicated their strong support for localization, particularly important data.

What is personal information, important data, and CII?

The CSL defines personal information as “all kinds of information ... that taken alone or together with other information, is sufficient to identify a natural person’s identity...”. Subsequent regulations have clarified – as expected and in line with other regulators around the world – that these include names, identification (ID) numbers, emails, and biometric data. Important data, on the other hand, is a concept is unique to China and is therefore harder to grasp for foreign businesses. The CSL vaguely refers to it as “data that are closely related to national security, economic development, and social public interests...”. Subsequent draft guidelines have provided a little more clarity on what is important data for individual sectors, and it now includes a wide variety of topics, such as chemical factory layouts, clinical trial data, and geo-information.

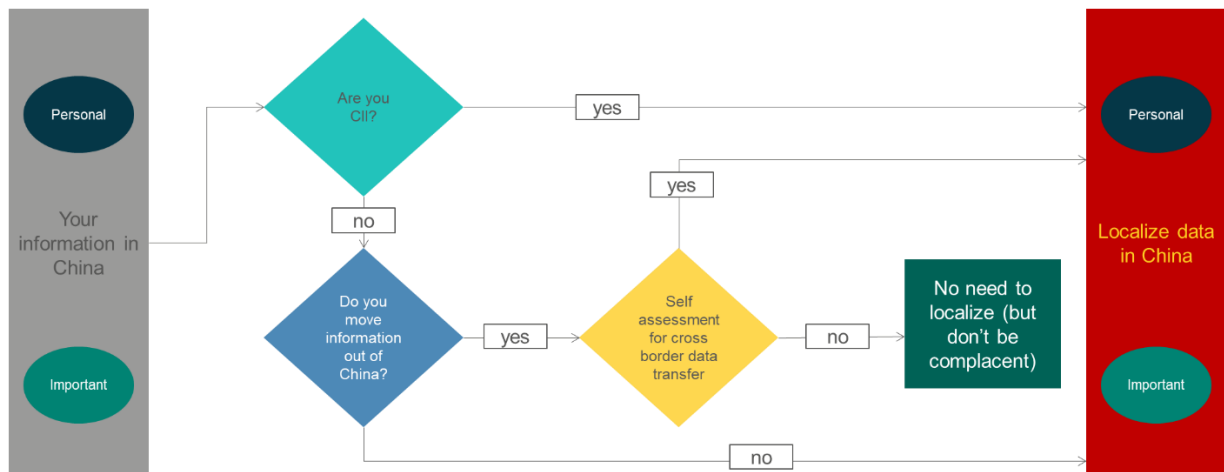
CII operators, who are required to localize personal and important data, are those that provide “... key protection to critical industries and fields like public communications and information services, power, transportation, water, finance, public service, electronic governance... and other critical information infrastructure that if destroyed, loses function, or leaks data might seriously endanger national security, national welfare, and the people’s livelihood, or the public interest...”. Examples of potential CII include companies in the sectors specifically listed as CII in the CSL and other regulations (such as finance and industrial manufacturing), but also those with large amounts of personal data (such as retail or consumer products) or with sensitive important data (such as those in chemicals, pharmaceuticals and medical devices).

Do you have personal or important data? If so, where is it?

Companies need to understand if they have personal and important data and where and how that data is stored. This is generally not a straightforward process; data targeted by Chinese regulators can be found in various departments – marketing, sales, legal, IT, and HR, R&D, to name a few. The following decision flow graph outlines the overall process.



Decision flow on data localization in China



Am I CII?

Step one is determining if your company is CII. The lack of transparency around CII identification makes this an exceptionally difficult exercise, but there are some indicators regarding what is considered 'critical' in the eyes of the regulators as outlined above.

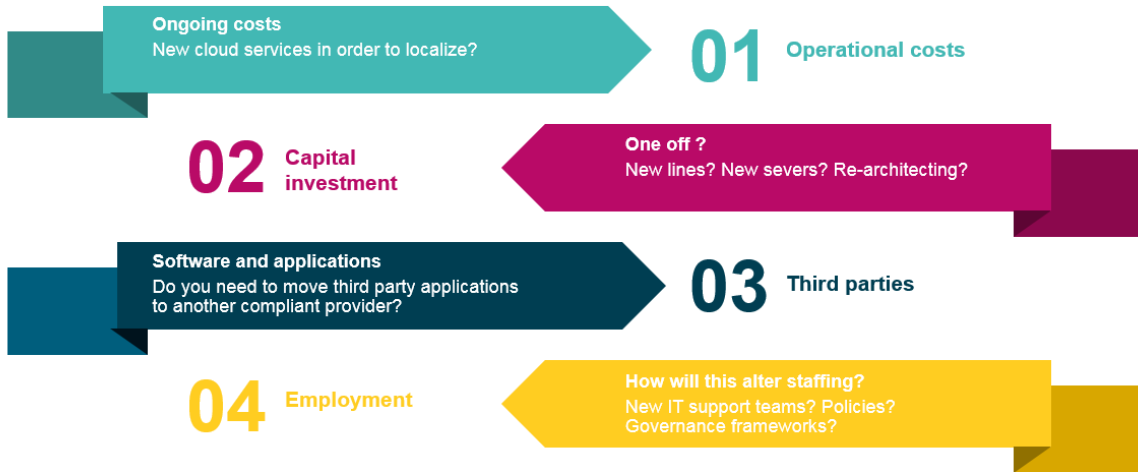
Can I transfer this data outside of China?

Both CII and network operators must conduct the self-assessment found in the cross-border data transfer guidelines to determine whether data can be transferred outside of China. The self-assessment scores data on possible impact from data transfer, level of controls, and where that data is headed. Final scores of "high" or "very high" means that the data should not be transferred outside of China. The self-assessment will provide companies with greater clarity on how to achieve a score that allows for transfer.

How do I keep it and what are the data localization costs?

Localization can take many forms, with various costs involved. These include operational, capital investment, third party and employment costs. The following chart outlines key questions around localization.

► What are the cost implications?



Government recommendations

On May 24, 2018, AmCham Shanghai and Control Risks held a briefing with members ranging from large MNCs to small medium-sized enterprises (SMEs) to discuss these developments and potential advocacy that AmCham can conduct with the Chinese government on the data localization issue.

Recommendations include:

- **Greater transparency on CII identification and localization scope:** the current scope for data localization is currently broad and ambiguous. The government should provide more clarity on CII status and the type of data that is targeted for localization.
- **Greater transparency on localization timing:** Considering the significant time required to fully complete localization, government regulators should provide an indication of when the cross-border transfer regulation will be finalized. Following finalization, regulators should provide a grace period of at least one year so companies have adequate time to comply.
- **Independent cross-border data transfer reviews:** Government should allow the majority of companies to conduct self-assessments, and where an audit is truly necessary, appoint a recognized internationally-certified independent third-party auditor to conduct the assessments.

About the Author

Control Risks is a specialist risk consultancy. Based in multiple offices on all continents, we are committed to helping our clients build organizations that are secure, compliant and resilient in an age of ever-changing risk and connectivity.

We believe that responsible risk taking is at the core of our clients' success. We have unparalleled experience in helping clients solve the challenges and crises that arise in any ambitious organization seeking to convert risk into opportunity globally. The insight and depth of experience we have gained over more than forty years proves invaluable in giving our clients the intelligence they need to grasp opportunities with greater certainty. Learn more at www.controlrisks.com.

For inquiries, please contact Jim Fitzsimmons (Jim.Fitzsimmons@controlrisks.com) or Carly Ramsey (Carly.Ramsey@controlrisks.com).

About the GPS Program

AmCham Shanghai's Government Policy Support (GPS) Program is dedicated to helping members navigate the impact of industrial policy on business. Drawing from the knowledge of industry experts in business, academia, and government, GPS provides members with the latest policy developments and valuable insights into how these translate into commercial opportunities and challenges for companies.

This report is the second in a series of quarterly reports available exclusively to GPS Program members. For more information, please contact daniel.rechtschaffen@amcham-shanghai.org.

