The Imminent Expansion of Data Localization in China?

Authors:

Kate Yin
Partner, Fangda Partners
kate.yin@fangdalaw.com

Gil Zhang
Partner, Fangda Partners
gil.zhang@fangdalaw.com

With contribution from Huihui Li and Jianqi Yang
If one thing should keep foreign companies in China on alert, it is the restrictions on cross-border data transfer under Chinese law. Since the passage of the Cyber Security Law (the “CSL”), Chinese regulators such as the Cyberspace Administration of China (“CAC”) have been attempting to address the concerns arising from cross-border data transfers in the past five years. These rule-making efforts by Chinese regulators to curb the cross-border transfer of personal information and important data are still ongoing as of the date of this article. The application of these draft rules appears to be universal, meaning that no company is exempt. Most of these drafts authorize regulators to control cross-border data transfer through pre-transfer approval or pre-transfer filing.

The latest effort is that CAC finally released the much-awaited prescribed template for the cross-border data transfer agreement (the “Draft China SCC”) in the draft Provisions on the Prescribed Agreement on Cross-border Data Transfer (the “Draft China SCC Provisions”) for public consultation on June 30, 2022. The Draft China SCC Provisions correlates to the final Measures on Security Assessment on Cross-border Data Transfer (“Security Assessment Measures”) that have been released by CAC on July 7, 2022 as well as Article 38 and 40 of the Personal Information Protection Law (the “PIPL”). The Security Assessment Measures and the Draft China SCC Provisions provide a fairly low bar for government approval for cross-border data transfers, which is as low as transferring the sensitive personal data of 10,000 individuals across the border. At the current stage, companies are commonly concerned with the sudden changes in the law and whether they would be able to obtain government approval for their cross-border data transfers if such approval were to be required by March 1, 2023 as the end of grace period provided under the Security Assessment Measures.

In addition to companies operating in sectors already adopting data localization requirements before the implementation of the CSL, such as banking financial institutions, medical institutions, and autonomous driving and car hailing companies, many companies not subject to these sector-specific rules in China are still expecting Chinese regulators to pull the trigger and to prompt them to press the button for data localization. While some companies are still in wait-and-see mode, other companies in heavily regulated sectors are either preparing localization plans to mitigate risks associated with uncertainty in obtaining government approval to export data, or preparing a response plan that can function as a road map to comply with changes in law during a grace period.
Data Localization Requirements under Chinese Laws

The general legal requirements on data localization and cross-border data transfer under the CSL, the Data Security Law (the “DSL”) and the PIPL mainly apply to personal information and important data. Those requirements require that personal information and important data collected or generated in China must be locally stored and that such data may not be transferred cross-border unless the transfer is necessitated by genuine and legitimate business demands and a prior security assessment has been completed. These requirements apply to critical information infrastructure operators (“CIIO”) and personal information handlers who process personal information over a certain volume. While the volume threshold is currently unclear, it is expected that CAC will clarify the threshold in the final version of the Draft Security Assessment Measures.

In addition to these general data localization requirements, there are specific data localization rules for companies operating in highly regulated sectors. These specific data localization requirements vary sector by sector. Some requirements are imposed at the organization level (i.e., all of the company’s information systems must be localized in China), or are imposed at the business system or data category level. The following chart lists the data localization requirements in some highly regulated sectors.

<table>
<thead>
<tr>
<th>Regulated Sectors</th>
<th>Localization Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>a) Banks shall localize the processing of personal financial information.</td>
</tr>
<tr>
<td></td>
<td>b) Credit investigation agencies shall localize the processing of the credit investigation information that is collected in the business operation.</td>
</tr>
<tr>
<td></td>
<td>c) Securities companies shall localize the servers for their online securities information systems that contain sensitive data such as client information.</td>
</tr>
<tr>
<td></td>
<td>d) Private investment fund service agencies shall localize the servers for their information systems used in the processing of their core business in China as well as the relevant data collected from such business (such as client data and business data).</td>
</tr>
<tr>
<td>Medical and healthcare</td>
<td>a) The processing of human genetic resources, healthcare big data and population demographic data shall be localized, and cross-border transfer of such data requires government approval/assessment.</td>
</tr>
<tr>
<td>Mapping and surveying</td>
<td>a) Internet map service providers shall store mapping data (e.g., GPS coordinates) in servers in China.</td>
</tr>
<tr>
<td></td>
<td>b) Online taxi booking platform operators shall localize the processing of personal data and business data collected or generated in China.</td>
</tr>
<tr>
<td>Online publishing</td>
<td>a) Online publishing service providers shall localize servers and equipment relevant to their online publishing business in China.</td>
</tr>
</tbody>
</table>
Extent of Localization in China

Data localization will generate added costs and require continuous investments in a business's China infrastructure. A copy of data in China can be accomplished by opting for cloud services in China in addition to the current choice of servers. A “full stack” data localization would be challenging as this means that all of the servers and information systems would need to be in China.

For the automotive industry, Chinese regulators have specified the scope of important data that shall be localized in China, including the storage and processing of that data. The scope of that data includes geographic information, traffic and people flows, economic data, vehicle charging network data, as well as personal information involving more than 100,000 individuals. Companies in the automotive industry need to deploy onshore information systems to process this important data.

For banks, in general, cross-border transfer of personal financial information requires prior “application” with industry regulators. As for the nature of such application, i.e., government approval or pure consultation, it may depend on the specific context and details of the cross-border data transfer.

In addition to following the clear localization requirement for human genetic resource data, many pharmaceutical companies are also considering locally storing a copy of any data collected by their China businesses in anticipation of changes in law and because of the uncertainty with obtaining government approval when required. Many big pharma companies are also pushing their CRM and primary HCP data providers to localize their servers in China.

In addition, Chinese regulators are prioritizing compliance with China’s Multiple-level Protection Scheme of Cybersecurity (“MLPS”). As a practical issue, when conducting an MLPS filing, a company may be required to migrate some information systems or servers to China, otherwise the MLPS testing agency would not have any control management systems, or related technical and management measures in China to grade and test.

Other than monitoring for changes in law, many companies have or are preparing the “break glass” protocol to respond to legal requirements or to Chinese regulators’ requests that require government review of cross-border transfers or require the localization of all data or the retention of a data copy in China. Considering that companies may need significant time to discuss, decide on, and implement a solution to address data localization requirements, some companies are proactively maintaining onshore servers copies of data related to their China business. For these onshore servers, companies not only may self-maintain these local servers, but may also, considering the market practice, consider using domestic service providers or using foreign-brand service providers who partner with Chinese service providers to provide local servers.
Data provision to foreign judicial bodies or law enforcement agencies

Though many legal uncertainties still exist, the disclosure of data (including both personal information and important data as well as other data to be further clarified by Chinese regulators) to foreign judicial bodies or law enforcement agencies is prohibited unless approved by the competent Chinese regulator in advance. Chinese regulators have not yet released implementation measures explaining how companies can obtain pre-approval, nor have they determined which regulators will be coordinating or frontloading the request for approval for now. These uncertainties prompt foreign companies to store data in China and to avoid sending servers containing personal data cross-border for forensic purposes.

While the restriction on cross-border data transfer seems imminent, it is necessary for companies to complete data mapping exercises for China-related data at a granular level and to establish different protocols for different data processing scenarios.