China released its “Standard Contractual Clauses” (SCC) for public consultation

Authors:

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

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

With contribution from Patrick Guo and Jianqi Yang
On June 30, 2022, the Cyberspace Administration of China (CAC) finally released the much-awaited prescribed template for the cross-border data transfer agreement (the “Draft China SCC”) as part of the draft Provisions on the Prescribed Agreement on Cross-border Data Transfer (the “Draft Provisions”) for public consultation. The consultation period ends on July 29, 2022. The Draft China SCC does not distinguish between controller-to-processor and controller-to-controller transfers and is expected to apply to every cross-border transfer of personal information. The Draft China SCC includes many provisions that resemble the controller-to-processor module of the EU SCC. This article examines the Draft China SCC and provides updates on the new requirements in the Draft Provisions.

1. Scenarios where China SCC can be used

Article 38 of the Personal Information Protection Law (the “PIPL”) requires that any transfer of personal information from China to another country must have one of the following: personal information protection certification for both the data exporter and the data importer, government-led security assessment, the conclusion of China SCC, or other legal formalities as provided by Chinese laws. Among these mechanisms, the Draft China SCC has been most welcome by many companies because it may be easiest to implement due to the uncertainty in obtaining a favorable security assessment and the difficulty and cost of having both data exporter and data importer being certificated by the PRC government.

However, in contrast with the EU SCC, the Draft China SCC seems to be applicable in fairly limited scenarios only when all of the following conditions are met (Article 4 of the Draft Provisions):

(a) the personal information handler ("PI Handler") has not been approached and designated the Chinese regulators as an operator of critical information infrastructure;

(b) the volume of personal information processed by the PI Handler does not reach one million individuals;

(c) the cumulative number of individuals whose personal information has been transferred by the PI Handler overseas since January 1 of the previous year has not reached 100,000; and

(d) the cumulative number of individuals whose sensitive personal information has been transferred overseas by the PI Handler since January 1 of the previous year has not reached 10,000.

For many data heavy sectors, such as retail, online services, banking, medical services, and other B2C services, one million individuals’ personal information is already a fairly low bar, let alone the threshold of 100,000 and 10,000 for cumulative transfers of personal information. For companies that have plants in China or employ over 10,000 employees, the cross-border transfer of employees’ personal information also may not be able to use China SCC because the personal information to be transferred and processed outside China normally will include sensitive personal information.
Under the PIPL, if a cross-border data transfer requires the government-led security assessment, then neither the SCC nor the certification can be used in lieu of such security assessment. As the CAC in the Draft Provisions seems to be reiterating the “one million individuals” threshold for triggering the government-led security assessment requirement, data-heavy companies that are hesitating on enacting their data localization plans may now have to re-evaluate the risks with further delay given the Draft Provisions.

Further, companies should monitor how personal information volume is calculated, i.e., whether the calculation will be conducted on an enterprise-level regardless of context, data subjects, systems or data sources (such as cloud services that act as processor/entrusted parties). For example, if a company uses a CRM and a data service with servers outside China that involve uploading data to the CRM, the company is likely to use China SCC for filing. However, it is not clear for now whether the CAC will aggregate all the data transferred outside China in various filings of China SCCs.

2. China version of transfer impact assessment

The Draft Provisions reiterated that PI Handlers must conduct a self-assessment to review the compliance with laws in the cross-border data transfer.

The assessment must address the following (article 5 of the Draft Provisions):

(a) the lawfulness, legitimacy and necessity of the purpose, scope and means of personal information processing activities by the PI Handler and the foreign recipient;

(b) the quantity, scope, category and sensitivity of personal information to be transferred outside China, as well as the risks to the legitimate rights and interests of the data subject as a result from the cross-border data transfer;

(c) the responsibilities and obligations that the foreign recipient undertakes to the PI Handler, as well as whether the managerial and technical measures adopted by the foreign recipient are adequate to ensure the security of transmission of personal information;

(d) the risks of data breach, data damage, data tampering, data abuse and other risks exposed to data that has been transferred to foreign recipient, as well as whether data subjects can successfully exercise their data subject rights;

(e) the impact on the performance of China SCC as a result of the policies, laws and regulations on personal information protection of the country or region where the foreign recipient is located; and

(f) other factors that may affect the security of cross-border data transfer.
Most of these assessment factors echo the self-assessment requirements under the draft Measures on the Security Assessment of Cross-border Data Transfer (the “Draft Security Assessment Measures”) released on October 29, 2021 by the CAC. Looking at the above assessment factors, the approach resembles the EU GDPR’s transfer impact assessment.

Given that one of the assessment factors is whether laws in other jurisdictions will impact the performance of the China SCC, it is likely that going forward companies in China will need to obtain local counsel’s opinion on whether local laws will restrict the foreign data recipient from performing the China SCC. However, it is unclear for now whether the local counsel’s opinion needs to be included in China’s transfer impact assessment and subsequently filed with the local CAC.

3. Filing of China SCC

The Draft Provisions propose that the PI Handler must file its use of prescribed agreement with the CAC’s local branch at the provincial level within 10 working days after the effective date of the prescribed agreement. The report of transfer impact assessment, along with the signed China SCC, must also be filed with the local CAC.

Because the SCC filing is not an approval, the Chinese regulators will not be able to review the substantive contents of the report of transfer impact assessment and reject the SCC filing. Although the Draft Provisions provide that the failure to file the Draft China SCC is a violation the PIPL, the CAC may need to reconcile this requirement with the PIPL because the PIPL does not require filing for China SCC in its Article 38.

If the requirement on the filling of China SCC is enforced, MNC affiliates and subsidiaries in China should consider using the China SCC for filing instead of filing the entire intragroup transfer agreement.

4. Frequency of filing and Validity of China SCC

Given that one of the thresholds for using the China SCC is the number of individuals whose personal information the foreign data recipient has received since January 1 of the previous year, it appears that the PI Handler must refile the China SCC every time when the said calculation period lapses. Having said that, it remains unclear on the calculation period to a certain extent. For example, if the Draft Provisions were to come into force in 2023, when calculating the number of individuals whose personal information is involved in the cross-border data transfer, does January 1 of the previous year refer to January 1 of 2022? If this is the case, such means of calculation may violate the general principle of lex retro non agit (law isn’t retroactive).
Moreover, as required by Article 8 of the Draft Provisions, any change to the quantity of data to be transferred overseas as agreed in the China SCC has to be filed with the CAC. It is unclear for now whether the CAC can accept a filing with an inexact volume or range of personal information, particularly in the context where the cross-border data transfer is expected to occur on ongoing basis rather than a one-time data transfer with an exact quantity of personal information, such as moving a server outside China or using a cloud service with a server outside China.

Another issue arising from the application threshold is whether the China SCC would automatically become invalid once the cumulative number of individuals whose personal information is transferred reaches the threshold for government-led security assessment.

According to Article 6 of the Draft Security Assessment Measures, PI Handlers are required to file a data transfer agreement containing security protection obligations and duties for assessment. The CAC likely expects that the PI Handler and the foreign data recipient will use the China SCC for this contract arrangement. The Cyber Security Standard Practical Guidance – Security Certification Specification on Cross-border Transfer of Personal Information issued on June 24, 2022, which is the first guidance relating to the certification mechanism, also proposed that a binding agreement or instrument for cross-border data transfer is necessary for obtaining the personal information protection certification.

5. Questions for further clarification

Whilst the Draft Provisions as well as the Draft China SCC respond to and clarify some legal uncertainties, various questions require the CAC’s further clarification. For example, will the Draft China SCC apply to a controller-to-controller data transfer? What if the foreign data recipient as data controller refuses to accept certain controller provisions such as audit cooperation with data subject requests and supervision acceptance from the Chinese regulators? How the China SCC can be used for processor-to-controller type of transfer? Can the China SCC be amended as per the negation by the contracting parties?

The Draft China SCC requires the foreign data recipient to accept the CAC’s supervision and to take remedial measures as required by the PRC government. Does this mean that foreign data recipient needs to periodically report to Chinese regulators its compliance with Chinese laws and measures to safeguard the data? This acceptance of Chinese regulators’ supervision may be a concern to certain foreign companies, particularly those with no business presence in China.
<table>
<thead>
<tr>
<th>Location</th>
<th>Address</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beijing</td>
<td>27/F, North Tower, Beijing Kerry Centre, 1 Guanghua Road, Chaoyang District, Beijing 100020, China</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tel: +86 10 5769 5600 Fax: +86 10 5769 5788</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guangzhou</td>
<td>17/F, International Finance Place, 8 Huaxia Road, Zhujiang New Town, Guangzhou 510623, China</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tel: +86 20 3225 3888 Fax: +86 20 3225 3899</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td>26/F, One Exchange Square, 8 Connaught Place, Central, Hong Kong</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tel: +852 3976 8888 Fax: +852 2110 4285</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shanghai</td>
<td>24/F, HKRI Centre Two, HKRI Taikoo Hui, 288 Shi Men Yi Road, Shanghai 200041, China</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tel: +86 21 2208 1166 Fax: +86 21 5298 5599</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shenzhen</td>
<td>17/F, Tower One, Kerry Plaza, 1 Zhong Xin Si Road, Futian District, Shenzhen 518048, China</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tel: +86 755 8159 3999 Fax: +86 755 8159 3900</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

www.fangdalaw.com