Baker McKenzie FenXun.

Client Alert

July 2022

# China: Draft China SCCs and pertinent rules released - Last piece of the puzzle for cross-border data transfer?

## In brief

On 30 June 2022, the Cyberspace Administration of China (CAC) released the draft Rules concerning the Standard Contract for Cross-Border Transfer of Personal Information ("**Draft Rules**") together with the draft Standard Contractual Clauses (China SCCs) for public consultation. The China SCCs for cross-border transfer of personal information are one of the three mechanisms for transferring personal information outside of China as stipulated in the Personal Information Protection Law of China (PIPL). The Technical Specifications for Security Certification of Cross-border Processing of Personal Information ("**Certification Specifications,**" a document without the force of law or regulation) and the final version of the Measures for Security Assessment of Transferring Data Abroad ("**Security Assessment Measures**") were also issued in the past few weeks, with the latter one being released by the CAC on 7 July 2022 , and they are intended to provide for the detailed implementation rules and guidelines concerning the other two mechanisms for cross-border transfer of personal information. Once finalized, the Draft Rules will become the "last piece of the puzzle," and the Chinese regulators will have relatively clear rules and guidelines concerning the cross-border transfer of personal information which will enable it to roll out the complete suite of the legal mechanisms for cross-border transfers of personal information in accordance with the PIPL around the first anniversary of the promulgation of the PIPL.

### In this issue



## Scope of application and proposed conditions for the use of the China SCCs

The Draft Rules propose the use of the China SCCs by certain personal information processors (PIPs) (as defined under the PIPL, a term akin to "data controller" under the General Data Protection Regulation, GDPR) or data exporters located in China as a legal mechanism to transfer outside of China personal information of individuals residing in China, if **all** of the stipulated criteria are met:

1. the PIP is not a critical information infrastructure operator (CIIO),
2. the PIP processes personal information of fewer than 1 million individuals residing in China,
3. since 1 January of the previous calendar year, the PIP provides personal information of fewer than 100,000 individuals residing in China to a foreign jurisdiction, **and**
4. since 1 January of the previous calendar year, the PIP provides sensitive personal information of fewer than 10,000 individuals to a foreign jurisdiction (collectively, the "**Proposed Conditions**").

This means that, if a PIP does not satisfy any of the Proposed Conditions, it will not be eligible to use the China SCCs and will need to resort to other transfer mechanisms as provided under Article 38 of the PIPL, for instance, by completing the mandatory security assessment administered by the CAC or obtaining the certification for personal information protection from a CAC-certified institution.

The Draft Rules set out the basic conditions and quantitative thresholds for using the China SCCs, but how the Proposed Conditions should be interpreted and applied are not crystal clear. For instance, an underlying question arises as to whether the thresholds of 1 million individuals (whose personal information is processed by a PIP), 100,000 individuals and 10,000

individuals (whose personal information is to be exported by a PIP during the relevant time period) under the Proposed Conditions should be calculated on the basis of each data flow, product line or entity, although a literal reading of the Draft Conditions suggests that the quantitative thresholds should be applied on an entity basis. In addition, a typical question which most multinational companies (MNCs) doing business in China may ask is: if we have multiple corporate entities in China under the same group that transfer data abroad to the headquarters overseas (to the same recipient basically) and the number of individuals whose personal information is exported by each entity is below the 100,000 or 10,000 threshold, but the aggregate number of individuals whose data is exported by all China entities (taken as a whole) during the applicable time period exceeds the 100,000 or 10,000 threshold, would each or some of these China entities be eligible to use and rely on the China SCCs for cross-border transfer of personal information? If each member of the group company is treated as an independent PIP under the Draft Rules, we believe that the aggregate number of individuals whose personal information is being exported should be calculated on the basis of each legal entity. Further, the Proposed Conditions provide that the time period for calculating the number of individuals in China whose data are being exported runs from 1 January of the preceding calendar year. The most likely interpretation of the said time period is that if these conditions are fulfilled concurrently in any two consecutive calendar years, a China SCCs-based contract for the export of personal information can be used.

Although the quantitative thresholds (1 million, 100,000 and 10,000) proposed under the Draft Rules are in line with those under the Security Assessment Measures, how the China SCCs are to be aligned with the mandatory security assessment administered by the CAC for cross-border data transfer (CBDT) outside of China needs to be clarified. Specifically, if, by reason of business expansion or growth, the number of individuals whose personal information are being processed by a PIP reaches 1 million, or if such PIP exports personal information above the 100,000 threshold or sensitive personal information above the 10,000 threshold in a certain two-year period resulting in the Proposed Conditions no longer being satisfied, should the PIP terminate the China SCCs-based contract and suspend CBDT immediately until it has applied for and passed the CBDT security assessment administered by the CAC? If this is the CAC's intention, then the normal business operations of the PIPs could be significantly affected. Therefore, it remains to be seen whether a grace period will be granted by the CAC to facilitate the transition to avoid business disruption or suspension that results from the termination of data export.

Another practical point arising from the Draft Rules is whether an entrusted party (i.e., a term equivalent to "data processor" under the GDPR) located in China can use the China SCCs to transfer personal information outside of China, as the Draft Rules and the China SCCs explicitly define the party located in China that transfers personal information outside of China (i.e., the data exporter) as a PIP. There could be scenarios where the data exporter in China acts as an entrusted party of a foreign recipient (who is the data controller) which collects and exports data of individuals in China for and on behalf of the foreign recipient. It would not be in line with the legislative intent if an entrusted party in China would not be allowed to rely on the China SCCs for CBDT even if it fulfills the Proposed Conditions.

According to Clause 1 of the China SCCs, the term "overseas recipient" refers to any organization or individual located outside of China that receives personal information from a PIP. Unlike its EU counterparts, the China SCCs do not distinguish a controller from a processor in using the term "overseas recipient," and therefore the China SCCs have not included different modules for the controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller scenarios.

## Structure and key provisions of the China SCCs

The Draft Rules propose the inclusion of the following provisions in the China SCCs:

1. the basic information of the data exporter and the overseas recipient, such as name and contact;
2. the purpose, scope, type, sensitivity, quantity, method, retention period, storage location, etc. of the personal information being transferred abroad (to be detailed in Annex 1 of the China SCCs);
3. the respective responsibilities and obligations of the data exporter and the overseas recipient to protect personal information, as well as the technical and management measures taken to prevent security risks that may arise from the export of personal information (Clauses 2-3 of the China SCCs);
4. the impact of the personal information protection policies and regulations of the country or region where the overseas recipient is located on the compliance with the terms of the standard contract (Clause 4 of the China SCCs);
5. the rights of data subjects, and the ways and means to protect such rights (Clause 5 of the China SCCs); and
6. other terms such as remedies, termination, liability and dispute resolution (Clauses 6-9 of the China SCCs).



© 2022 Baker & McKenzie FenXun Shanghai | 2

The China SCCs contain an annex whereby the parties may supplement other contractual provisions if needed. However, it is proposed in the Draft Rules that any other contract concluded between the data exporter and the overseas recipient concerning export of personal information outside of China should not conflict with the China SCCs. Clause 9 of the China SCCs further stipulates that the clauses of the China SCCs shall prevail in case of conflict between the China SCCs and other agreements that the parties have concluded. Therefore, while the parties are free to supplement the China SCCs with more detailed provisions concerning their respective roles, obligations and responsibilities, such supplementary provisions may not override the standard clauses in the China SCCs.

The main obligations of the data exporter under the China SCCs are as follows:

1. to ensure that the personal information is collected and processed according to applicable laws, and to adhere to the data minimization principle in respect of data export;
2. to comply with the notification and consent requirements under the PIPL;
3. to notify data subjects of their right as a third-party beneficiary under the China SCCs;
4. to make reasonable efforts to ensure the overseas recipient's compliance with the China SCCs and to take technical and management measures such as encryption, anonymization, de-identification, access control, etc.;
5. upon overseas recipient's request, to provide a copy of the relevant legal provisions and technical standards;
6. to respond to inquiries from regulators (the overseas recipient may also respond to such inquiries but the data exporter is the party that is obligated to provide a response);
7. to have conducted a Data Protection Impact Assessment (DPIA) (as defined below) according to applicable laws;
8. to provide a copy of the China SCCs to data subjects upon request (such copy could be redacted for trade secret protection);
9. to have the burden of proof with respect to compliance with the China SCCs; and
10. to provide to the regulators the materials or audit reports of overseas recipient to prove compliance of the China SCCs.

Insofar as the overseas recipient is concerned, its main obligations stipulated under the China SCCs are as follows:

1. to process personal information pursuant to requirements (with respect to processing purpose, scope, etc.) as set out under the China SCCs;
2. to provide a copy of the China SCCs to data subjects upon request (such copy could be redacted for trade secret protection);
3. to adhere to the data minimization principle in respect of data export;
4. to store the personal information for the minimum period of time necessary to achieve the processing purpose, and to delete or anonymize the personal information after the processing purpose is achieved unless separate consent is obtained;
5. to ensure security of personal information by (i) taking effective technical and management measures, and (ii) applying appropriate authorization and access control within organization;
6. in the event of data leakage, (i) to promptly take remedial measures, and (ii) to notify the data exporter and report to the Chinese regulators pursuant to laws;
7. NOT to (further) transfer personal information to any third party located outside China, unless certain requirements are met, including:
    a. there are genuine commercial needs for such transfer;
    b. the notice and consent requirements under the PIPL for transfer of personal information to another PIP have been satisfied;
    c. a written contract has been concluded with the third party to ensure a level of personal information protection not lower than that required under the PRC laws; and
    d. a copy of the said written contract has been provided to the data subjects.
8. when entrusted by a data exporter to process personal information, to obtain prior consent from the data subject when further entrusting a thirdparty sub-processor to process personal information;
9. to ensure compliance with the PIPL in respect of the automated decision-making rules, such as ensuring transparency, non-differential treatment, etc.;


© 2022 Baker & McKenzie FenXun Shanghai | 3

10. to undertake to provide all necessary information to the data exporter to prove compliance with the China SCCs, including permitting the data exporter to conduct audit on its data and files;
11. to keep records for at least three years regarding its personal information processing activities; and
12. to agree to be subject to the supervision of the Chinese regulators, including responding to inquiries, cooperating with inspections, etc.

As the China SCCs do not distinguish between the respective roles of the data exporter and the overseas recipient, the respective obligations and responsibilities stipulated in the China SCCs for each of the data exporter and the overseas recipient would be equally applicable. Conceivably, the parties will be allowed to specify their respective roles through supplementary provisions to the China SCCs. However, due to the stringent requirement that the standard clauses of the China SCCs would always prevail, the parties' ability to deviate from the obligations and responsibilities listed above to reallocate their respective obligations and responsibilities through supplementary provisions might be limited.

## Filing requirement and DPIA

The Draft Rules on China SCCs introduce a key requirement (which is unseen in other jurisdictions) that the contract for the export of personal information concluded based on the China SCCs needs to be filed with the provincial office of the CAC within 10 business days after the contract comes into effect. This filing requirement would not dictate the effectiveness of the contract and export of personal information could be initiated once the contract comes into effect (before the completion of filing with the CAC). It is also proposed in the Draft Rules that should there be a change to any key items in relation to the exported personal information (e.g., purpose of export, scope and types of exported personal information, level of sensitivity of exported personal information, retention period or storing location of exported personal information, change of purpose of processing by overseas recipient) or a change to the personal information protection laws, regulations and policies of the jurisdiction where the recipient is located which may have an impact on the rights and interests of the data subjects, the contract needs to be updated, re-executed and re-filed with the CAC.

It is noteworthy that the Draft Rules on the China SCCs require a PIP to file with the CAC the "DPIA report regarding the export of personal information together with the executed contract. Essentially, the DPIA needs to be completed by the PIP before concluding the China SCCs-based contract and it should ensure consistency between the assessment report and the information in the executed contract.

The requirement for PIPs in China to conduct a DPIA with respect to the export of personal information is based on Article 55 of the PIPL. Therefore, this requirement as proposed in the Draft Rules is not new. The DPIA proposed in the Draft Rules is also substantively similar to the self-assessment on the export of personal information as provided in Article 5 of the Security Assessment Measures. Nevertheless, based on the Draft Rules, the DPIA in relation to the conclusion of the contract for the export of personal information will need to cover a broader range of aspects than what is stipulated in the PIPL and the Security Assessment Measures. For instance, a DPIA, pursuant to the Draft Rules, is to cover the impact of the personal information protection laws, regulations and policies of the jurisdiction where the overseas recipient is located on the performance of the contract for the export of personal information concluded on the basis of the China SCCs, which is understood as comparable to the EU Transfer Impact Assessment introduced by the Schrems II judgment. If this requirement is kept in the final version of the Draft Rules, it would mean that performing a nuanced analysis of the level of compliance with the China data protection laws (especially the PIPL) in the overseas recipient's jurisdiction would be necessary.

## Potential liability for breach of the filing requirement

While the filing of the contract for the export of personal information with the provincial office of the CAC is not a condition precedent to the effectiveness of the contract, failure to comply with the filing requirement could result in legal ramifications based on the Draft Rules.

It is proposed in the Draft Rules that the CAC or its local offices at the provincial level can take enforcement actions against a PIP and order the PIP to make rectifications pursuant to the relevant provisions of the PIPL, if (i) the PIP fails to complete the filing with the CAC or submits false materials or information when making the filing, (ii) the PIP fails to perform the duties or obligations provided in the China SCCs-based contract executed by the PIP which causes harm to the rights and interests of data subjects, or (iii) there exists other circumstances that adversely impact the rights and interests of data subjects. In case of failure to rectify the



© 2022 Baker & McKenzie FenXun Shanghai | 4

non-compliance by the PIP, CAC can order the PIP to suspend the export of personal information and impose penalties according to the PIPL.

It should be noted that criminal liabilities could be imposed in severe circumstances where the non-compliance constitutes criminal offences, such as the crime of seriously infringing upon personal information of citizens, the crime of illegally collecting human genetic resource data, etc., as provided under the *Criminal Law* and other applicable PRC laws and regulations.

## Brief comparison with the EU Standard Contractual Clauses ("EU SCCs")

In general, the China SCCs share considerable similarities with the EU SCCs with respect to substantive requirements and obligations, including, among others, data minimization, storage limitations, documentation and audit, protection of data subject rights, etc. Further, both the China SCCs and the EU SCCs recognize protection over third-party beneficiaries, and the protections are substantially the same. Additionally, they both require the data exporter and overseas recipient to assess the impact of the overseas laws on the performance of the SCCs before carrying out a CBDT.

However, as mentioned above, the EU SCCss have four modules designed for different data transfer scenarios based on the nature of the roles and responsibilities of the parties (namely, from data controller / processor to data controller / processor), whereas the China SCCs seem to adopt a one-size-fits-all approach. In addition, the EU SCCs allow contracting parties to modify the standard terms (subject to the regulator's approval) for more flexible data protection provisions, whereas it remains unclear whether the China SCCs would allow such modification and whether the filing requirement for the China SCCs could be used as a mechanism to allow flexibility. Last but not least, the China SCCs provide that they are governed by the PRC law, while the EU SCCs afford more flexibility as to the choice of governing law (depending on the module applicable, the governing law may or may not have to be the law of a EU/EEA country).

For MNCs that have rolled out intra-group transfer agreements based on the EU SCCs, their China subsidiaries would need to regularly assess if they are eligible to use the China SCCs in respect of their export of personal information outside of China and, conclude contracts for such CBDT based on the China SCCs if applicable, instead of simply supplementing the existing intra-group transfer agreements. Accordingly, it would be inevitable for these Chinese subsidiaries to consider how to ensure consistency and harmony between the China SCCs-based contract for the export of personal information and the intra-group transfer agreement.

## Looking Forward

As the Security Assessment Measures will come into effect on 1 September 2022, we expect that the China SCCs and the Draft Rules will also be finalized in the coming months so that they can complement each other to enable the Chinese regulators to have full coverage of regulation over cross-border transfers of personal information outside of China. There is a possibility that a similar transition period as stipulated under the Security Assessment Measures will also be put in place for companies to digest the requirements, assess their eligibility for using the China SCCs and take steps to conduct the DPIA and conclude the contracts. We also expect that the CAC will launch an online portal on which the filing of the China SCCs-based contracts can be carried out.



© 2022 Baker & McKenzie FenXun Shanghai | 5

## Contact Us

**Zhenyu Ruan**
Senior Counsel, Shanghai
zhenyu.ruan@bakermckenziefenxun.com

**Yangdi Zhao**
Associate, Shanghai
yangdi.zhao@bakermckenziefenxun.com

**Cora Wu**
Associate, Shanghai
cora.wu@bakermckenziefenxun.com

© 2022 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the this Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.