Chinese standard contractual clauses for cross-border personal information transfer – an update

February 2023

Executive summary

According to the China Personal Information Protection Law ('**PIPL**') and related regulations, standard contractual clauses ('**Chinese SCCs**') prescribed by the Chinese government can be used as a mechanism for cross-border data transfers from China if Chinese government approval (i.e. a 'security assessment') is not required. The Chinese SCCs were issued on 22 February 2023 by the Chinese cybersecurity regulator, Cyberspace Administration of China ('**CAC**'), and will become effective on 1 June 2023. For existing personal data outbound transfers, there is a six-month grace period (to 1 December 2023) for compliance.

The Chinese SCCs are provisions to be entered into by the companies (data controllers) and the overseas recipients, governing the rights and liabilities of the companies, the overseas recipients and the individuals when the companies transfer personal data of the individuals to the overseas recipients. Contracts between the companies and the overseas recipients concerning the cross-border transfer of personal information must not conflict with the Chinese SCCs[1].

Unlike the EU General Data Protection Regulation (GDPR), both the signed Chinese SCCs and the cross-border impact assessment must be submitted to local Chinese regulators within the time limits, as discussed below.

Who may use the Chinese SCCs?

Only companies meeting each of the following conditions may rely on the Chinese SCCs alone to transfer personal information outside of China:

(1) It is not a critical information infrastructure operator;

(2) It processes the personal information of fewer than one (1) million individuals;

(3) It has not cumulatively provided overseas personal information of 100,000 individuals since 1 January of the preceding year; and

(4) It has not cumulatively provided overseas sensitive personal information of 10,000 individuals since 1 January of the preceding year ('sensitive personal information' refers to the personal information that, once leaked or illegally used, can easily lead to the infringement of personal dignity of natural persons or the harm on personal and property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts, and other information, as well as the personal information of minors under the age of 14).

[1] The Chinese SCCs can be incorporated by companies into their contractual arrangements with other parties or can be standalone documents. The text of the SCCs may not be altered, except to increase the level of protection for the data. For example, parties may supplement the SCCs with additional clauses or incorporate them into a broader commercial contract, as long as the other contractual provisions do not contradict the SCCs, either directly or indirectly, or prejudice the rights of data subjects.

It is important to note that China law also sets out other requirements, such as all outbound transfer of Important Data must first obtain government approval. (Important Data: Data that may endanger national security, economic operation, social stability, public health, and safety once they are tampered with, destroyed, leaked, or illegally obtained or used illegally).

Impact assessment and recordal

The existing requirement that companies must conduct impact assessments prior to transferring personal data cross-border is stressed in the Chinese SCCs as the impact assessment results need to be submitted to the local provincial-level cyberspace authority within ten working days from their effective date. The impact assessment results are required to be kept for at least three years.

The Chinese SCCs must be recorded with the local provincial-level cyberspace authority within ten (10) working days from their effective date.

In case of any substantive change, the impact assessment must be repeated and the Chinese SCCs must be updated and re-recorded.

Rights of individuals

The company must notify each individual that it is a third party beneficiary under the Chinese SCCs, with such Chinese SCCs provided to the individual upon request.

The Chinese SCCs reiterate various requirements already set out in the PIPL, including those in respect of automated decision making and transparency (the company and the overseas recipient need to explain the rules of data processing to the individual). The communications with the individual should be clear, easy to understand and thorough. The Chinese SCCs also reiterate the individual's right to access, copy, amend and delete his/her data. If the individual's request is denied, he/she should be given reasons and informed of complaint and litigation options.

Obligations of overseas recipients

The overseas recipient is subject to the supervision of Chinese regulators (including complying with their orders and providing written proof of having taken compliance steps).

The overseas recipient must keep records of its data processing for at least three (3) years.

Onward transfer

An onward transfer of personal data by the overseas recipient needs to meet additional requirements, such as meeting the necessity requirement and obtaining an additional unbundled consent (termed 'Separate Consent') from the individual.

Country risk assessment

The Chinese SCCs also consider whether the jurisdiction of the overseas recipient accords a level of protection essentially equivalent to that required by the PIPL. The company and the overseas recipient need to conduct prior assessment, among other things, of the law for protection for personal information in the overseas jurisdiction.

Contact person

The overseas recipient should designate an internal contact for addressing inquiries and complaints from the individuals and the contact details should be notified to the individuals.

Governing law and dispute resolution

The governing law of the Chinese SCCs is China law. Disputes arising from the Chinese SCCs may be handled by arbitration (including by arbitration bodies under the New York Convention (Convention on the Recognition and Enforcement of Foreign Arbitral Awards)) or by litigation (in a Chinese court).

The individual may lodge complaints with Chinese regulators or sue in China, and the company and the overseas recipient are jointly liable to the individual under the Chinese SCCs.

Next step

All outbound transfer of personal information from China, including intercompany transfer to headquarters outside of China, must proceed using one of the three mechanisms prescribed under China law.

- Government approval (security assessment) (see earlier newsflashes here and here)
- Certification by a professional institution designated by the Chinese government (see earlier newsflash here)
- Entering into the Chinese SCCs

(The deadline for compliance if government approval (security assessment) is needed being 1 March 2023)

China has been very aggressive with enforcement of its data rules. Responsible individuals may be fined as well as blacklisted from holding important positions for a period of time. The Chinese criminal authorities reported that they have arrested 17,000 people in 2021 alone for data violation.

The first step foreign businesses should take is to understand if and how the new China requirements apply to them. They need to assess whether they need to obtain Chinese government approval for their outbound sharing or transfer of data, including conducting impact assessment. If they need to obtain Chinese government approval, they should submit the applications with the provincial level regulators (see earlier newsflashes here and here). Otherwise, they may choose to proceed with the certification or the Chinese SCCs mechanism. In the case of the Chinese SCCs mechanism, they can finalize the Chinese SCCs and execute or they can incorporate the Chinese SCCs into their existing agreements.

We have a large and experienced team of cybersecurity and data privacy professionals assisting companies with outbound data transfers using the prescribed mechanisms. Please let us know if you have any questions.

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

Tiang & Partners

Chiang Ling Li
Partner
Tiang & Partners
+852 2833 4938
chiang.ling.li@tiangandpartners.com

PwC Hong Kong

Kristine Chung
Partner
PwC Hong Kong
+852 2289 1902
kristine.ky.chung@hk.pwc.com

www.pwc.com
www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所