China: Draft SCCs Released - Time to Focus on Overseas Data Transfers

4 July 2022

By: Carolyn Bigg | Fangfang Song | Venus Cheung

The China draft SCCs have been published, but may not provide the easy approach to cross border transfers of Mainland China personal data we have hoped to. Requirements to file the SCCs or PIIA for each transfer with the regulator, to undertake mini transfer impact assessments upon changes to a recipient country's data laws, and regulator powers to suspend cross border data transfers as a sanction for non-compliance with the PIPL, mean that this is not just a case of updating intra group, vendor and business partner agreements to include the new SCCs.

The Cyberspace Administration of China (CAC) issued the Draft Provisions on Standard Contracts for Cross-border Transfer of Personal Information (Draft SCCs Provisions) on 30 June 2022. The Draft SCCs Provisions provide clarification on how the SCCs may be implemented by organisations as one of the mechanisms for overseas data transfer under the Personal Information Protection Law.

The Draft SCCs Provisions include template SCCs. The template SCCs appear to be influenced by GDPR, and a number of clauses are aligned with the GDPR. Notably, the Draft SCCs Provisions do not distinguish C2C/C2P transfers.

- Organisations may rely on SCCs only if all of the below conditions are satisfied:
  - it is not a critical information infrastructure operator (CIIO);
  - it processes personal information of no more than one million individuals;
  - it has transferred personal information of no more than 100,000 individuals since January 1 of the previous year (i.e., potentially up to a two-year period); and
  - it has transferred sensitive personal information of fewer than 10,000 individuals since January 1 of the previous year (i.e., potentially up to a two-year period).

The above threshold is generally aligned with the draft Measures on Security Assessment of Overseas Data Transfer released last year. That means, if the data transfer does not satisfy any of the above conditions, the organisation is not able to rely on SCC. Instead, a CAC-conducted security assessment must be carried out for overseas data transfer.

- The SCCs should include the following provisions:
  - basic information of the organisation and the overseas recipient, including but not limited to names, addresses, names and contact information of contact persons, etc.;
  - the purpose, scope, type, sensitivity, quantity, method, retention period and place of storage of the personal information;
  - the responsibilities and obligations of the organisation and overseas recipient, as well as technical and management security measures; and
  - the impacts of the data privacy laws and regulations of the destination country on the SCC;
  - data subject rights, approaches to exercise such rights; and
  - remedy, rescission of contract, liability, disputes resolution, etc.

- The Draft SCCs Provisions reiterate that, before transferring personal data outside of Mainland China, a personal information impact assessment should be conducted. (Of course, explicit, separate consent, must be also obtained.)
- The SCCs should be filed with the local CAC within 10 days after taking effect. In addition, the PIIA should also be filed. This suggests, although the drafting is not explicit on this point, that copies of each and every SCCs signed on a per transfer/contract basis must be filed.
- New SCCs should be signed in each of the below circumstances:
  - change of data processing activities, including change of purpose, scope, type, sensitivity, quantity, method, retention period and place of storage, method of overseas recipients to process personal information, or extension of retention period of personal information;
  - change to the data privacy laws and regulations of the destination jurisdiction that may impact the rights and interests of individuals. This appears to involve a “light” version of GDPR/Schrems II transfer impact assessment; or
  - other circumstances that may affect the rights and interests of individuals.
- The local CAC (provincial level or above) is entitled to suspend the overseas transfer of personal data by any organisation if the local CAC discovers that the actual transfer does not comply with the relevant cross border data transfer rules. This is a significant incentive for organisations to comply, as the operational and contractual risks for organisations having to suspend cross data transfer, including investment to setting up a solely in-country infrastructure, would no doubt be more costly than a regulatory fine.

Separately, for those organisations preferring not to use the SCCs, an alternative route would be for the organistion to get overall accreditation for its global data transfers from a certification body. Separate draft guidelines outlining the procedure to do this were published last month for public consultation.

AUTHORS

Carolyn Bigg
Partner
Hong Kong | T: +852 2103 0808
carolyn.bigg@dlapiper.com

Fangfang Song
Consultant
Beijing | T: +86 10 8520 0600
fangfang.song@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
Hong Kong | T: +852 2103 0808
venus.cheung@dlapiper.com