SQUIRE PATTON BOGGS

China Releases the Standard Contract on Personal Information Export

Asia Pacific – March 2023

On February 24, 2023, the Cyberspace Administration of China (CAC) released the Standard Contract of Personal Information Export (PRC SCCs) and the Measures on the Standard Contract of Personal Information Export (Measures).

These apply to the transport (transfer) of any personal information from China except where even stricter measures are required (such as for) critical information, large volume and/or sensitive personal information). The PRC SCCs and Measures are effective on June 1, 2023 for any new transfers. A six-month grace period will apply to any transfers made before June 1, 2023. Companies need to act as soon as possible to ensure compliance. The main aspects of the PRC SCCs are detailed below.

Is it New?

Overall, the PRC SCCs and Measures are similar to the previous draft released for public comment in June 2022, including the introduction of a controversial filing requirement that goes beyond the provisions in the Personal Information Protection Law (2021) (PIPL). We covered this in a prior Privacy World blogpost. This obligates the Personal Information Processor (data controller) exporting from China any personal information collected from within, even for just a single person's data, to execute the required PRC SCC with the recipient prior to transfer and to file it, along with a detailed Personal Information Protection Impact Assessment (PIPIA) report with the Chinese government.[1] We note that the new Measures do not alter the need under Article 39 of the PIPL to obtain the separate, informed consent of the individual for the export. The PIPL provides a very few specific exceptions that may apply. The PIPL also designates that the export should only occur where the controller 'really needs to provide the personal information outside the territory of the People's Republic of China due to business or other needs…' (Article 38).

Key Elements of the PRC SCCs

PRC SCCs, not for all – Stricter rules, requiring a mandatory security assessment by the CAC, are required for personal information with a state concern or depending on the volume of data. However, the PRC SCC terms apply to all other controllers located in China that want to export personal information from China and are not subject to the CAC-required security assessment. The mandatory CAC security assessment is required when any of the following take place:

- The controller is a critical information infrastructure operator (CIIO), which means it is processing information deemed critical to the security of China, such as, for example, defence, transportation, telecom, health, finance, energy and anything that may involve the national security and public interest of China
- The volume of personal data processed by the data controller exceeds one million individuals
- The amount of personal information exported by the data controller exceeds 100,000 individuals' data since January 1 of the preceding year
- If more than 10,000 individuals' sensitive personal data has been exported by the controller since January 1 of the preceding year

Please read our Privacy World blogpost for more about the required CAC security assessment.

As above, the newly issued Measures and PRC SCCs apply to the rest of any desired personal data exports. Please note that a data "export" refers not only to the physical movement or transfer of personal data from China to outside of China, but also includes personal data stored in China that is *accessible* by parties outside of China. Under the PIPL (Article 38), as long as the data controller is not subject to mandatory CAC assessment (as above), instead of choosing to submit to a voluntary CAC evaluation, it may instead choose to utilize the PRC SCC method as the basis of personal information export. Such an export now requires the following:

- Execution of the PRC SCCs with any receiving party (including affiliates, inter-company, or third parties) and ensuring the obligations set forth therein are followed
- Completion of a PIPIA
- Filing both of these documents with the CAC within 10 days of execution of the PRC SCCs

Taking them in reverse order, we address each:

- **Filing requirements** – The Measures require Controllers to file with the provincial department of the CAC within 10 working days after a PRC SCCs take effect, (i) the executed PRC SCC, and (ii) a PIPIA relating to the data export. Should any changes in the transfer occur thereafter, an amended PRC SCC and PIPIA report should be refiled. While the Measures state it as a "filing(备案)" process, it is unclear whether the CAC will conduct a substantive review on the filing materials with scrutiny and require rectification in case the exportation is deemed inappropriate.
- **Data export PIPIA** – While the requirement of PIPIA for data export exists under the PIPL, the Measures expand the scope of assessment to not only cover the principles set forth in the PIPL (i.e. necessity and legitimacy of the transport (transfer), risks to personal interests and security measures posed by the transport (transfer)), but now also includes assessing the potential impact of the foreign legal environment and the effectiveness of a challenge available to data subjects in the foreign jurisdiction. The PIPIA may be conducted by the Controller itself with assistance from outside service providers.

[1] Under the PIPL, controllers may choose to go through a "personal information protection certification" conducted by qualified agencies, if entering into a Standard Contract is not desired.

It should be noted that the PIPIA is not a mere formality. The PIPIA is essentially a process of doing a compliance gap assessment and making improvements or remedial actions throughout the organization. Among other things, the final PIPIA report should sufficiently demonstrate that the scope the personal information export satisfies the "minimum and necessary" principle, and that sufficient security measures have been taken to minimize the security risks and impact on individuals. In our experience, it could take several months to finalize a PIPIA report of this nature, depending on the complexity of the data flow. Further, keep in mind that the PIPIA must be filed with the authorities.

- **Provisions in the PRC SCCs** – The Measures state that Chinese controllers and overseas recipients must strictly follow the PRC SCCs template provided in the Measures, and that the parties shall not enter into any agreement conflicting with the PRC SCCs, although there is an area in which to add clauses of a nature that do not contradict the proscribed clauses.

  Below we have highlighted some of the most notable provisions in the PRC SCCs:

  - **Obligations of the overseas recipients** – The PRC SCCs impose very detailed obligations on overseas recipients, including the requirements on minimum retention period, access control, notification to data subjects and the Chinese authority in case of a security incident, conditions on third-party on-transfers and subprocessing, record-keeping, etc. Many of these are similar to those under the EU Standard Contractual Clauses, but in some ways, far exceed them. For example, the PRC SCC is not separated into controller-to-controller, controller-to-processor or other arrangements. Instead, only one PRC SCC is available. This means, for example, that the export recipient must notify not only the data controller, but also the Chinese data privacy authority and the individual data subjects of any data breach or security incident. Importantly, the PRC SCCs also include the obligation of the overseas recipient to be supervised by the Chinese authorities with regard to any inquiries, inspections and/or implementing any orders by the authorities.
  - **Impact of the foreign legal environment** – Under the PRC SCCs, the parties are required to evaluate the laws and regulations of the country in which the overseas recipient is located, and both parties are required to make the representation that the performance of the PRC SCC will not be negatively impacted by the laws of the foreign jurisdictions.
  - **Data subjects as third-party beneficiaries** – It is specifically provided in the PRC SCCs that a data subject is a third-party beneficiary. Individuals have the right to make data subject requests (including requesting a copy of the PRC SCCs) to the controller or to the overseas recipient directly. In addition, data subjects may claim against either or both parties to perform their obligations related to individuals' rights under the PRC SCCs, or to bring a lawsuit against either or both parties at a Chinese court in relation thereto.
  - **Effectiveness** – The PRC SCCs shall be governed by Chinese law, and its terms shall prevail over any other agreements reached by the parties with regard to the subject matter. Disputes between the exporting party and the overseas recipient are to be resolved by mutual negotiation, but failing that, by a competent Chinese court or by arbitration (with arbitration in China being preferred, but the option to list another forum where the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention) is recognized).
  - **Details on personal information processing** – The details on the exportation activity should be set forth in an exhibit to the PRC SCCs, including the purpose of the export, types and volume of personal information being exported, subprocessing or transfer, retention period and location of storage. The change of the foregoing should result in an update to the PIPIA report, the amendment to the Standard Contract, and refiling of both documents.

Implementation date and grace period. The Measures will take effect from June 1, 2023, for new transfers. Transfers that have occurred prior to June 1, 2023, will have a grace period of six months before being adequately documented and in compliance.

Given the extent of these obligations, if you haven't already, we strongly recommend that companies, especially multinational corporations, take actions to immediately evaluate their cross-border data transfers from China and, as needed, 1) complete the PIPIA on personal information exports, 2) enter into the PRC SCC with the overseas recipients, and 3) file the required documentation with the CAC within the required period. The APAC members of our Global Data Practice can assist you in managing this process. For more information, contact the authors or your relationship partner in the firm.

Contacts

Ju (Lindsay) Zhu
Partner, Shanghai
T +1 86 21 6103 6303
E lindsay.zhu@squirepb.com

Katherine Fan
Associate, Shanghai
T +86 21 6103 6323
E katherine.fan@squirepb.com

Scott A. Warren
Partner, Tokyo and Shanghai
T +81 3 5774 1800
E scott.warren@squirepb.com

Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Nicholas Hiu Fung Chan
Partner, Hong Kong
T + 852 2103 0388
E nick.chan@squirepb.com