DS NEWSLETTER savoir faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

What's new about cross-border data transfer from China in 2022?

CHINA

BACKGROUND

Since the implementation of *PRC Cyber Security Law* in 2017, foreign invested enterprises have been concerned about the requirements of data localization, and they have been wondered that how the cross-border data transfer security assessment will be carried out. Last year, *PRC Data Security Law* and *Personal Information Protection Law ("**PIPL**")* were promulgated and took effect, but they remain vague on this topic.

To solve this issue, Cyberspace Administration of China ("**CAC**"), competent authority in charge of cross-border data transfer, released *Measures for the Security Assessment of Cross-border Data Transfers* ("***Measures***") on July 7th, 2022, which already took effect on September 1st, 2022.

Measures clarify in brief the scenarios and conditions where cross-border data (including personal information, "**PI**") transfer is subject to security assessment conducted by CAC, how to apply for the security assessment, what materials to be submitted, timeframe and consequence of failing the security assessment. In practice, in order to facilitate this new formality for applicants, CAC already provides a detailed guide (in Chinese, http://www.cac.gov.cn/2022-08/31/c_1663568169996202.htm) and some official templates for application of security assessment. Some municipal and provincial offices (Beijing, Tianjin, Shanghai, Zhejiang province, Jiangsu province and Hebei province) of CAC also disclose their consultation hotlines.

Obviously, the Chinese regulatory framework on cross-border data transfer is rapidly forming. In view of this background, the following Q&A will present the important messages sent by some recent legal updates on cross-border data transfer.

***

1. Question: what types of activities are considered as cross-border data transfers?

   (1) For data collected and/or generated by data controllers during the operation in China, it is transmitted to and/or saved overseas by data controllers;

   (2) For data collected and/or generated by data controllers, it is saved in China by data controllers, but it can also be accessed, queried, retrieved, downloaded and/or exported by institutions, organizations and/or individuals from overseas; and,

   (3) Other cross-border data transfer activities as stipulated by CAC.

2. Question: is CAC security assessment applicable to all cross-border data transfers?

In fact, not all cross-border data transfers are subject to CAC security assessment. Only those meet at least one of the conditions set by *Measures* will have to do so (see Question No. 3 for details).

For cross-border data transfer activities, they should be also compliant per other applicable laws (e.g., PIPL, and other industry-oriented laws and regulations, etc. See Question No.8 for information about cross-border PI transfer activities which do not trigger CAC security assessment).

3. Question: who needs to apply for security assessment to CAC?

For data controllers who provide important data and/or PI collected and/or generated in China to overseas, if they meet any of the following conditions, they should apply for security assessment to CAC:

(1) Data controllers provide important data to overseas;

(2) Critical information infrastructure operators ("**CIIO(s)**") or PI controllers who process the PI of or more than 1 million individuals provide PI to overseas (this condition focuses on the total volume of PI processed by the CIIOs/PI controllers and despite the volume of PI to be transferred to overseas);

(3) Since January 1st, 2021, PI controllers who have accumulatively provided PI of or more than 100,000 individuals or sensitive PI of or more than 10,000 individuals to overseas, provide PI to overseas (this condition focuses on the accumulative volume of PI processed by PI controllers over a definite timeframe and despite the volume of PI to be transferred to overseas);

(4) Other situations that require the declaration of cross-border data transfer security assessment as stipulated by CAC.

4. Questions: what about cross-border data transfer activities have been started before the effective date of *Measures* (September 1st, 2022)?

CAC gives a grace period for these data activities. If they meet any of the aforementioned scenarios and/or conditions in Question No. 3, the relevant data controllers should complete the security assessment before March 1st, 2023.

5. Question: what needs to be submitted for the security assessment to CAC?

(1) Copy of the unified social credit code of the institution/enterprise;

(2) Copy of the identity document of the legal representative;

(3) Copy of the identity document of the agent in charge of the formality for the applicant;

(4) Power of Authorization to the agent (CAC official template);

(5) Application Letter for cross-border data transfer security assessment (CAC official template);

(6) Copy of the contract(s) and/or other legal documents concluded between the data exporter and the data importer;

(7) The report on self-assessment of the risks in the cross-border data transfer (CAC official template) and the self-assessment should be completed 3 months in advance of the application of CAC security assessment;

(8) Other materials as required for the security assessment by CAC.

6. Question: how long does the security assessment take?

After receiving the complete and correct application materials, the competent CAC office will inform the applicants in writing whether to accept it within 7 working days. During this period, applicants may be required to supplement or correct the application materials. If the submitted materials do not meet the requirements, CAC office may terminate the assessment. In normal cases, the assessment will be completed within 45 working days after acceptance. In complicated cases, this period may be extended.

7. Question: how long will the security assessment result be valid?

The assessment result will be valid for 2 years. Be there any major change of the cross-border data transfer activity, the data controller should re-apply for security assessment.

8. Question: what about cross-border PI transfer activities which do not trigger CAC security assessment?

According to *PIPL*, before any cross-border transfer, PI controllers should:

(1) ensure that they have the legal basis for the relevant PI processing (e.g., processing PI of employees for the purpose of HR management, and processing PI of an individual who is as a party to a contract and for the purpose of signing the contract etc.); and,

(2) conduct PI protection impact assessment and obtain the separate consent of data subjects if needed.

After the above tasks, theoretically speaking, if a cross-border PI transfer does not trigger a mandatory CAC security assessment, the PI controller/PI exporter may choose to legitimize the transfer by concluding a Chinese "Standard Contractual Clauses" ("**Chinese SCC**") with the PI importer or by other ways.

In practice, it seems that the Chinese SCC are currently the most feasible way. A recent draft regulation indicates that CAC may implement the Chinese SCC as the standard contract for cross-border PI transfer set forth by *PIPL*. The Chinese SCC draft has already been released by CAC. In the future, PI exporters would be required to conclude the SCC with the PI importers and record-file the Chinese SCC with CAC as well.

9. Question: what is the content of the Chinese SCC?

The Chinese SCC (remain draft version at the moment) clarify the compliance requirements for PI controllers as PI exporters and the obligations for PI importers, and it would function in a way similar with the SCC under GDPR.

To be more specific, the Chinese SCC include the basic information, rights and obligations of PI exporters and PI importers, the details of the processing of PI to be transferred (e.g., purpose, scope and categories of PI, sensitivity and volume of PI, method

of processing, etc.), the impact of the laws and regulations of PI importers' country/region, and the protection of the rights of the data subjects. Per the current Chinese SCC draft, PI exporters and PI importers may agree on other matters in addition to the aforementioned items.

***

In practice, so far it seems that, there has not been many administrative punishment cases in charged by CAC concerning cross-border data transfer, but the situation would be changed soon. Because on September 8th, 2022, CAC issued *Provisions on Administration Law Enforcement Procedures of Cyberspace Administration Departments (Draft for comment)*. This *Provisions* will be the legal grounds for CAC to supervise and enforce the laws related to cyber content, cybersecurity, data security and PI protection.

In addition, as *Measures* are effective and the Chinese SCC are almost in place, we recommend that enterprises in relation to data processing activities to prioritize the compliance task of cross-border data transfer and assign dedicated professionals internally and/or externally to improve the situation as soon as possible.

For any additional information please contact:

ZHANGBeibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com