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

What to know about the Chinese Standard Contractual Clauses for Cross-border Personal Data Transfer?

CHINA

.

BACKGROUND

The Chinese Personal Information Protection Law ("PIPL") has been in effect for a year and a half, but the rules governing cross-border personal data transfer ("CBDT") had not been clear due to the lack of applicable and practical transfer tools. While the regulatory authority, the Cyberspace Administration of China ("CAC"), started implementing the CAC security assessment for important CBDT activities last year, transfer tools were not readily available for other CBDT activities, such as the transfer of employees' personal data in relatively small amounts for HR purposes.

(*Please check our previous newsletter "*What's new about cross-border data transfer from China in 2022?* to know the "*important CBDT activities*" which are mandatorily subject to the CAC security assessment.
English version: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%202209%20EN%20cross-border%20data%20transfer.pdf;
French version: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%202209%20FR%20cross-border%20data%20transfer.pdf)

WHAT'S NEW?

China has recently taken a significant step towards regularizing CBDT activities by completing transfer tools for data controllers. These tools include the CAC security assessment, the personal information protection certification, and the newly released Standard Contractual Clauses for Cross-border Transfer of Personal Information, also known as the Chinese SCC.

On February 24th, 2023, CAC released the Chinese SCC, which provides a set of contractual clauses to regulate the transfer of personal data from China to other countries. In addition, CAC has also issued the *Regulation on the Standard Contract for Cross-border Transfer of Personal Information* ("Regulation"), which outlines how the Chinese SCC will be implemented. The Regulation will come into effect on June 1st, 2023.

WHAT TO DO?

According to the Regulation, data controllers whose CBDT activities do not require a security assessment from the CAC must still complete the Chinese SCC with their data importers.

After concluding the SCC, data controllers are required to record-file the SCC and the Protection Impact Assessment ("PIA") report with the CAC within 10 working days of the Chinese SCC's effective date. This is a crucial step in ensuring compliance with the Chinese regulatory requirements on CBDT and avoiding potential legal risks.

It is important for data controllers to familiarize themselves with the available transfer tools and to assess if the Chinese SCC is a good choice for them; if so, they need to take necessary measures to comply with the Regulation before it comes into effect.

To that end, data controllers are advised to carefully review the Regulation and take necessary measures to comply with the record-filing requirements to ensure a smooth and compliant CBDT operation. Failure to comply with the regulatory requirements could result in fines, legal action, and damage to the company's reputation.

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject.

ANY "DEADLINE"?

The Regulation will come into effect on June 1st, 2023. Data controllers may wonder whether the Regulation will apply retrospectively to CBDT activities that began before this date.

According to the Regulation, data controllers will need to regularize both their current CBDT activities and new CBDT activities that start after June 1st, 2023, within a six-month grace period, or by December 1st, 2023.

HOW TO DO?

CBDT compliance requires both proactive internal support and external assistance in the long run, considering both mandatory requirements and practical needs.

Under the Regulation, data controllers are required to continuously supervise data processing activities to identify any factor that may affect the rights and interests of data subjects. If there are any material changes in the CBDT, data controllers should, again, conduct a PIA, conclude the Chinese SCC, and then have them record-filed with the CAC.

To meet these requirements, EU-background data controllers with a good data protection culture may make full use of their experience and practice in compliance under GDPR. However, proper implementation requires smooth communication between the Chinese local team and the headquarters, as well as a well-designed action plan. It is important to note that due to a lack of data protection practice in the past, the Chinese local team should firstly have an adequate level of awareness of data protection. Otherwise, they may find it challenging to turn policies into actions effectively.

AN EASY TASK IN PRACTICE?

CBDT compliance is not a one-time task, but an ongoing process. Data controllers should continuously evaluate the privacy risks and update their measures accordingly. This requires a proactive approach and a strong data protection culture within the organization. Data controllers may need to involve their legal, IT, and data protection teams to ensure comprehensive and effective measures. In addition, they may need to seek external assistance from professionals who are familiar with both Chinese regulations and international data protection standards.

Data controllers should not underestimate the importance of CBDT compliance and should take proactive measures to ensure they are in line with the regulations. By doing so, they can not only avoid potential penalties and reputational damage but also enhance the trust and loyalty of their customers.

THE FOLLOWING PROCEDURES ARE RECOMMENDED IN IMPLEMENTING THE CHINESE SCC AND ENSURING CBDT COMPLIANCE:

1. Providing training to improve and align data protection understanding is critical to ensure that everyone involved in the process understands the requirements and procedures;
2. confirm the person or department in charge of CBDT compliance to ensure that there is someone responsible for overseeing the process and ensuring that everything is done correctly;
3. Data mapping of current and new CBDT activities is also an essential step to ensure that all activities are identified and evaluated for potential privacy risks;
4. Conducting a PIA and preparing reports is critical to evaluate and mitigate privacy risks and ensure that adequate safeguards are in place to protect personal data;
5. Consulting professionals to check if the Chinese SCC is a suitable transfer tool, as there may be other transfer tools available that may be more appropriate for specific situations;

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject.

6. Negotiating and concluding the SCC with data importers is an important step to ensure that both parties understand their obligations and responsibilities under the Chinese SCC;
7. Recording filing the PIA report and the Chinese SCC with CAC before December 1st, 2023, is essential to ensure compliance with the Regulation;
8. Properly keeping the PIA reports for at least three years and monitoring the CBDT activities as required by the Regulation is also crucial to ensure ongoing compliance and to make sure that any changes to the activities are evaluated and addressed as necessary.

***

China's data protection laws have undergone significant changes in recent years, with the aim of fostering a strong data protection culture within organizations. Thus, data controllers are recommended to adopt a sustainable and comprehensive approach to keep a good balance between the budget and compliance.

Data controllers of B2C businesses may have already started their data protection compliance process one year or two years ago, because their business typically involves more complicated data processing activities, and the amount of data they handle can be quite large, which can trigger CAC security assessments. In 2023, it is imperative for B2B data controllers to implement measures and not wait any longer.

For any additional information please contact:

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

09, March 2023

The Newsletter is provided for general informational purposes only. Any information contained in this should not be construed as legal advice and is not intended to be a substitute for legal counsel on any subject.