CHINA EASES CROSS-BORDER DATA TRANSFER CONTROLS

On 22 March 2024, the Cyberspace Administration of China ("**CAC**") issued the official *Provisions on Promoting and Regulating Cross-Border Data Flow* ("**Provisions**") with immediate effect. The Provisions modify China's existing cross-border data transfer rules and introduce a number of exemptions following comments on its draft version released on 28 September 2023.

This Client Alert summarises the application of the three mechanisms available for transferring data out of China, as well as the positive developments that the Provisions have brought.

Editorial

FAN Jiannian, Partner
HAN Sufeng, Associate
TANG Jiale, Associate

BACKGROUND

In recent years, China has built up a comprehensive cross-border data transfer regime, most notably through the *Personal Information Protection Law* ("**PIPL**"), *Measures for the Security Assessment of Data Cross-Border Transfer* ("**Security Assessment Measures**"), *Measures on Standard Contracts for the Export of Personal Information* ("**Standard Contracts Measures**"), as well as accompanying regulations and guidelines.

Prior to the promulgation of the Provisions, personal information and "important data"[1] may be exported outside of China only after one of the following three procedures have been completed: (i) passing a security assessment led by the CAC ("**Security Assessment**"); (ii) obtaining a personal information protection certification issued by a specialised institution ("**Protection Certification**"); (iii) entering into a standard contract with the overseas recipient and filing the same with the provincial CAC ("**Standard Contract**").

Under the Security Assessment Measures, the Security Assessment was mandatory for transfers of the following types of data out of China:

(1) Important data;

(2) Personal information by (i) CII operators[2] or (ii) data processors that process the personal information of more than 1 million individuals;

[1] The concept of "important data" is introduced and regulated by the *Data Security Law* which provides that a catalogue of important data will be formulated by authorities. The *Security Assessment Measures* further define "important data" as data that, once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operations, social stability, or public health and security, etc.

[2] CII operators refer to operators of critical information infrastructure. Under the *Regulations on Security Protection of Critical Information Infrastructure*, "CII" refers to important network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government, and science and technology industry for national defense as well as other important network facilities and information systems which in case of destruction, functional loss or data leakage may result in serious damage to national security, the economy or public interest. The identification of CII will be determined by regulators and notified to operators.

(3) Personal information by a data processor that since 1 January of the previous year has transferred in aggregate (i) the personal information of over 100,000 individuals or (ii) sensitive personal information[3] of over 10,000 individuals; and

(4) Other data under other circumstances as determined by the CAC.

For other data falling outside these categories, data processors may choose either the Protection Certification or the Standard Contract before transferring data abroad.

In practice, the low trigger threshold, cumbersome procedures and unclear requirements associated with the three transfer options have created compliance challenges for multinational companies and their operations in China. In response to the State Council's call to promote foreign investment and address burdensome requirements for business operators, the CAC has finally adopted the Provisions to loosen cross-border data transfer requirements. In particular, the Provisions raise the threshold for triggering the Security Assessment and provide a number of exemptions to the three transfer mechanisms.

HIGHLIGHTS

Clarification And Relaxation For Security Assessment

The Provisions keep the restrictions imposed on CII operators for the transfer of important data and personal information, but for non-CII operators, the thresholds for the Security Assessment have been relaxed. Notably, the Security Assessment is no longer required for a data processor processing the personal information of more than 1 million individuals. This is a welcome development, as previously the simple holding of personal information of more than 1 million individuals in China for any length of time would require the Security Assessment, regardless of the actual volume of personal information to be transferred.

The Security Assessment now applies to non-CII operators when they transfer important data or non-sensitive personal information of more than 1 million individuals cumulatively, or when they transfer sensitive personal information of more than 10,000 individuals cumulatively. Furthermore, non-CII operators may opt for the Protection Certification or Standard Contract when cumulatively transferring non-sensitive personal information of 100,000 to 1 million individuals or sensitive personal information of up to 10,000 individuals.

In contrast to the Security Assessment Measures, the Provisions calculate the cumulative number of individuals starting from 1 January of the current year instead of the preceding year, offering a further relaxation of rules.

The table below summarises which of the three mechanisms applies in which cases (subject to the exemptions proposed by the Provisions as outlined below):

[3] According to the PIPL, "sensitive personal information" refers to personal information that, if disclosed or misused, could easily lead to the infringement of an individual's personal dignity or endanger the safety of persons and property. This includes biometric information, religious beliefs, specific identities, medical health, financial accounts, location and other information, as well as the personal information of minors under the age of 14. For more specific guidance on the identification of sensitive personal information, please refer to *The Information Security Technology — Personal Information Security Specification (GB/T 35273-2020)*.

Data Processor	Security Assessment	Protection Certification	Standard Contract
CII Operators	✓ Important data ✓ Personal information	Not applicable	
Non-CII Operators	✓ Important data ✓ Personal information, if the volume (cumulatively from 1 January of the current year) reaches the following threshold: - non-sensitive personal information of more than 1 million individuals, or - sensitive personal information of more than 10,000 individuals	✓ Personal information, if the volume (cumulatively from 1 January of the current year) reaches the following threshold: - non-sensitive personal information of 100,000 to 1 million individuals, or - sensitive personal information of up to 10,000 individuals	

In addition, the Provisions clarify that data processors will not need to pass the Security Assessment for reason of important data for cross border transfer of any data unless such data has been specifically categorised as important data by relevant departments or regions through notifications or announcements.

What is noteworthy is that the Provisions shall apply in case of any discrepancies between the Security Assessment Measures, Standard Contracts Measures and other relevant regulations.

Exemptions Proposed By The Provisions

The Provisions propose a complete exemption from the three transfer mechanisms under the following six circumstances:

(1) Data Category Exemption

Data that is generated in the course of international trade, cross-border transportation, academic cooperation, cross-border production or manufacturing, marketing and other activities that do not contain any personal information or important data.

(2) Overseas Data Exemption

Personal information that is collected and generated overseas by a data processor and transmitted to China for processing, when no domestic personal information or important data is introduced during the processing.

(3) Contract Exemption

Personal information that is “necessary” for concluding or performing under a contract to which an individual is a party, such as cross-border purchases, cross-border remittance, cross-border account opening, air ticket and hotel booking, visa application processing and examination services, etc.

(4) HR Management Exemption

Personal information of employees that is "necessary" for human resources management activities that are lawfully conducted in accordance with labour regulations and collective labour contracts.

(5) Emergency Exemption

Personal information that is "necessary" in an emergency to protect the life and health of individuals or the safety of property.

(6) Volume-Based Exemption

Non-CII operators providing non-sensitive personal information of fewer than 100,000 individuals outside China since 1 January of the current year.

The three necessity-based cases (items 3, 4 and 5 above) may cause practical challenges for business operations, as it is still unclear what constitutes "necessary".

Another point to note is that the Provisions require all cross-border transfers of sensitive personal information (even a small amount) to obtain a Protection Certification or Standard Contract (unless such information falls under exemptions 3, 4 and 5). Data processors should pay special attention to whether there is any sensitive personal information in their data transfers that does not fall under any of the above exemptions. For example, the ID numbers and bank account information of employees transferred abroad by the company are exempted, but the same information of contact persons from other cooperating parties (e.g. suppliers and clients) may not be. Thus, a Standard Contract should be concluded or a Protection Certification be obtained.

Free Trade Zones

The Provisions allow a free trade zone to formulate local preferential policies (negative list) to further relax cross-border data transfers in their respective jurisdictions. This is the first time that a negative list has been introduced in the regulatory regime for cross-border data transfers in China. Similar to the negative list adopted for foreign investments, data that falls beyond the scope of the negative list would not be subject to any of the three transfer mechanisms.

In this regard, the free trade zones in China are actively proposing regulations and documents to relax requirements for cross-border data transfers by companies registered in their jurisdictions. However, it remains to be seen how data flows from China outside the free trade zones into the free trade zones and then further out of China will be regulated.

Other Points

In contrast with the Security Assessment Measures, the Provisions extend the validity period for the Security Assessment from two years to three years, which may be further extended for another three years upon application before its expiry. The Provisions also emphasise the obligations of data processors that export personal information: They must notify the individuals, obtain separate consent, and conduct self-assessments [4] on their personal information protections.

[4] A self-assessment is required prior to applying for a Security Assessment with the CAC. For more information about the self-assessment, please see the Security Assessment Measures.

It is worth noting that on the same date, the CAC also issued the second edition of the Guidelines for Application for the Security Assessment of Cross-Border Transfers and Guidelines for Filing of the Standard Contract for Cross-Border Transfers of Personal Information, with the aim to optimise the application materials and simplify the procedures for the Security Assessment and Standard Contract filing

COMMENTS

To sum up, the Provisions will greatly reduce the compliance burden associated with cross-border data transfers, particularly for non-CII companies. In turn, this will also improve China's foreign investment environment. We recommend foreign investors to further evaluate their business operations based on the Provisions and update their compliance strategies for cross-border data transfers.

CONTACTS

Beijing

GUO MIN
guo@gide.com

DAVID BOITOUT
boitout@gide.com

Shanghai

FAN JIANNIAN
fan@gide.com

DAVID BOITOUT
boitout@gide.com

Paris

ANTOINE DE LA GATINAIS
gatinais@gide.com

CHARLES-HENRI LEGER
leger@gide.com

GUILLAUME ROUGIER-BRIERRE
rougier@gide.com

STÉPHANE VERNAY
vernay@gide.com

THOMAS URLACHER
urlacher@gide.com