GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity

March 2024

China Relaxes Requirements for Cross-Border Data Transfers

New provisions exempt data controllers from reporting to the Cybersecurity Administration in defined scenarios.

On March 22, 2024, the centralized regulator of cyber and data security, the Cybersecurity Administration of China (CAC), published the *Provisions on Promoting and Regulating the Cross-border Flow of Data* (New Provisions), relaxing the existing requirements relating to cross-border data transfers. The New Provisions took immediate effect on March 22, 2024.

Existing Obligations Regarding Cross-Border Data Transfers

Prior to the New Provisions, CAC published certain implementing regulations according to the *Data Security Law* (DSL*) and* the *Personal Information Protection Law* (PIPL) detailing the requirements for cross-border data transfers. These implementing provisions required data controllers to report or file their cross-border transfer case with CAC (CAC Obligations). Depending on the nature and volume of data involved, the original three CAC Obligations were triggered in the following scenarios:

(a) If the data controller was identified as a critical information infrastructure operator (CIIO), was holding personal data of at least 1 million individuals, or processed important data, the controller was required to submit a comprehensive report regarding its cross-border transfer case to CAC

and obtain clearance from the regulator (CAC Clearance) before the controller was permitted to export any such data outside China.

(b) If the controller was, in any period starting from Jan. 1 of the preceding year, exporting personal data of at least 100,000 individuals or sensitive personal data of at least 10,000 individuals, the controller was required to secure CAC Clearance.

(c) If the controller did not fall into either scenario identified in (a) or (b) above, the controller could elect to (i) enter into standard contract clauses (SCCs) published by CAC with the data recipient, and (ii) file the SCCs and a privacy impact assessment (PIA) analyzing the data transfer with CAC.[1]

The implementing regulations invited controversy from industries as such regulations would impose disproportionate obligations on data controllers on certain occasions. For example, pursuant to (a) above, any business holding personal data of at least 1 million individuals had to complete the lengthy CAC Clearance even if they were only exporting data of a limited number of individuals. Pursuant to (c) above, small businesses having only a handful of employees in China had to sign and file the SCCs and the completed PIA report with CAC if they transferred such employee data to affiliates abroad for HR or benefit purposes.

Relaxed Positions Under New Provisions

In September 2023, CAC proposed a draft transfer regulation relaxing the existing transfer rules by providing carveouts exempting data controllers from CAC Obligations. The New Provisions retain the substantial part of the exemptions proposed in the draft. We set forth details of the New Provisions below.

Safe Harbors from CAC Obligations

Article 5 of the New Provisions provides a "safe harbor" rule exempting data controllers from the CAC Obligations in each of the following situations:

(1) transfer of non-sensitive personal data of less than 100,000 individuals in any given year (provided the controller is not a CIIO);

(2) transfer of an employee's personal data that is necessary for HR administration according to a collective labor contract or an employment policy adopted according to law;

(3) transfer of personal data necessary for performing a contract with said individual, including for purposes of cross-border commerce, money remittance, opening bank accounts, air and accommodation booking, visa and exam services, etc.; or

(4) transfer of personal data necessary for protecting life and property security of a natural person in emergency.

[1] PIPL and CAC's implementing regulations provide an alternative to the SCC approach, where a data controller falling short of the scenarios identified in (a) or (b) can elect to complete a third-party certification regarding the cross-border transfer for its transfer of personal data to be legitimate under PIPL. Given that reliable third-party certifiers are limited in number, the "certification" approach is less utilized by most multinational companies. For completeness, the reference to "CAC Obligations" should include certification through third parties.

Note that exemptions (2) through (4) overlap with the non-consent legal bases as provided under Article 13 of PIPL, on which the data controller can rely to process and transfer data without consent. As a result, if a data controller satisfies the "necessity" justification and other conditions as stated in any of the applicable exemptions, that controller may be able to transfer and process the data without obtaining consent from individuals or complying with any of the CAC Obligations.

Exemptions (1) and (2) offer a solution to multinational companies operating in China who have a regular need to transfer personal data of their employees, vendors, customers, and other business partners for various business reasons. When relying on these exemptions, companies must adhere to the entire exemption, including the conditions attached. For example, with respect to exemption (2), the data overseas must be justified as necessary for human resources administration and there must be well-documented and duly approved employment policies supporting the transfer of data.

Limiting Applicability of CAC Obligations

Articles 7 through 9 of the New Provisions restrict applicability of CAC Obligations. Specifically, CAC Clearance is now required when:

(a) the data controller is a CIIO;

(b) the controller is transferring any important data; or

(c) the controller is, in any given year, exporting personal data of at least 1 million individuals or sensitive personal data of at least 10,000 individuals.

A data controller is required to sign the SCCs with the data recipient and file the SCCs and a PIA with CAC when (a) the controller is, in any given year starting Jan. 1, exporting personal data of at least 100,000 individuals but less than 1 million individuals, or (b) the controller is, in any given year starting Jan. 1, exporting any sensitive personal data (but of less than 10,000 individuals).

As compared to the original implementing regulations, the New Provisions limit the applicability of the CAC Obligations by (a) subjecting only data controllers transferring large volumes of data or sensitive data (if they are not CIIOs) to CAC Clearance, and (b) reducing the applicable time frame to calculate the requisite data volume from two years to one year, effectively raising the threshold for CAC Obligations. Article 9 of the New Provisions further extends the validity period of a CAC Clearance from two years to three years, reducing the administrative burden associated with reoccurring reporting obligations.

Assumption Regarding 'Important Data'

The term "important data" is undefined under the DSL, creating ambiguity and concern across industries and potentially subjecting the data controller to an array of enhanced cyber and data-related obligations (including obligating the data controller to complete a full CAC Clearance for transfers of such data outside of China). CAC has, on occasion, viewed "important data" like personal data existing in large volume and/or having other sensitive features. As a result, and depending on future CAC decisions, data controllers holding important data may be subject to future CAC Obligations.

The New Provisions allow data controllers to assume they are not transferring important data, and thus not required to obtain CAC Clearance, unless the relevant authority has "notified" them that they are processing important data or has publicly catalogued such data as important data. Businesses should still be mindful to monitor regulatory developments around "important data," as CAC and other regulators are

going full-speed ahead formulating industry-specific catalogues of important data or guidance to identify what constitutes important data.

B2B and Outsourcing Exceptions

Aside from the relaxed transfer requirements, the New Provisions clarify a few business scenarios where inquiries around CAC Obligations may arise. For example, Article 3 of the New Provisions make clear that data collected and processed in the course of cross-border trade, manufacturing, marketing, academic cooperation, etc. are not subject to CAC Obligations if no personal data or important data is involved (e.g., B2B transfers). Moreover, Article 4 exempts personal data "in transit" from CAC Obligations, meaning personal data collected outside China and processed within China for purposes of being transferred elsewhere are not subject to CAC Obligations, so long as the processed data is not combined with any China-originating personal or important data. This is often referred to as an outsourcing exception.

Conclusion

Multinational businesses should revisit their cross-border transfer activities in light of the New Provisions and assess whether the exemptions apply to them. Even if exempt from CAC Obligations, businesses transferring China-originating data overseas nevertheless must be mindful to comply with the other obligations under PIPL, including completing the required disclosure to and obtaining consent from the individuals, and conducting a PIA for the data transfer according to Article 55 of PIPL. Those businesses that have already submitted for CAC Clearance or filed the SCCs may elect to either continue the review or withdraw the case from CAC if justified under any of the stated exemptions under the New Provisions.

Authors

This GT Alert was prepared by:

- George Qi | +86 (0) 21.6391.6633 | qig@gtlaw.com
- Philip Ruan | +86 (0) 21.6391.6633 | ruanp@gtlaw.com
- Andrea C. Maciejewski | +1 303.685.7458 | maciejewskia@gtlaw.com
- Mike Summers | Resident Attorney | Denver