Skadden

# Cybersecurity and Data Privacy Update

November 7, 2023

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys on the last page or call your regular Skadden contact.



One Manhattan West
New York, NY 10001
212.735.3000

## China Intends To Ease Controls Over Cross-Border Data Transfers

### Executive Summary

On September 28, 2023, the Cyberspace Administration of China (CAC) published the draft Provisions on Regulating and Promoting Cross-Border Data Transfers (Draft Provisions). If adopted into law in their current form, the Draft Provisions would:

- Exempt a large number of companies that export data and other information from China in certain common business scenarios from otherwise mandatory data export requirements.
- Raise the minimum threshold for triggering the onerous Security Assessment requirement with the CAC.
- Limit the scope of "Important Data" (which is subject to higher scrutiny by PRC authorities) to data explicitly designated as such by authorities.
- Allow free trade zones to determine what types of cross-border data transfers are subject to mandatory data export procedures.

The introduction of the Draft Provisions indicates a willingness on the part of regulators to ease some the more onerous data privacy, administrative, commercial and human resource requirements that existing laws and regulations impose on both domestic and international business communities. It is an effort to improve the People's Republic of China's (PRC's) foreign investment environment to promote and attract increased foreign investment. No date has been announced for when the finalized provisions might be implemented.

### Background

The PRC's current data export compliance regime is primarily grounded in the Personal Information Protection Law (PIPL), which was enacted into law in November 2021, and subsequent accompanying regulations. Under the current regulatory framework, data handlers exporting data from the PRC are subject to one of three data export requirement schemes depending on the identity of the data handler and the nature and volume of the data: (i) Security Assessment by the CAC, (ii) Certification from a qualified institution, or (iii) Standard Contract, with language specified by the CAC.

As explained in our August 23, 2022, article "New PRC Regulations on Cross-Border Transfer of Data," the current legal landscape's unclear requirements, low trigger threshold, slow administrative procedures, severe consequences for non-compliance, and various practical challenges for multinational businesses have disincentivized foreign enterprises and investors from conducting business in the PRC.

The State Council, China's chief administrative authority, announced a new public policy initiative in August 2023 aimed at optimizing the country's foreign investment

environment. Responding to that and considering the feedback and concerns from companies about the compliance hardships engendered by the current regulatory regime, the CAC issued the Draft Provisions the following month with a truncated two-week public consultation period.

## Key Provisions

### Proposed Exemptions

The Draft Provisions start with a general statement that none of the Security Assessment, Certification or Standard Contract requirement schemes is applicable if the data to be exported was generated in activities such as international trade, academic cooperation, cross-border manufacturing or marketing that do *not* contain personal information or "Important Data." Specifically, the Draft Provisions propose a complete exemption from the three data export requirement schemes in the following circumstances:

1. It is necessary for the performance of a contract to which a data subject (*i.e.*, an individual to whom personal data relates) is a party (*e.g.*, cross-border purchase of goods, cross-border fund transfers, air tickets or hotel reservations and visa processing).
2. The exported data is (i) related to a company's internal employee data and (ii) necessary in accordance with the company's labor policies and rules formulated on the basis of a law, regulation or collective bargaining contract.
3. The expected cross-border transfer of data concerns fewer than 10,000 individuals' personal information within a calendar year.
4. The exported personal information is not collected or generated within the PRC.
5. The cross-border data transfers are necessary for protecting the health and property safety of an individual in an emergency.
6. The cross-border data transfers fall outside of free trade zones' Negative Data List.

While the exemptions help clarify the types of data and practices that would be exempt from the requirements of the Security Assessment, Certification and Standard Contract regimes, a number of points need to be clarified.

For instance, with respect to the second exemption, it is unclear what constitutes "necessary." Moreover, the Draft Provisions do not address whether companies may assert that they are exempt from the otherwise mandatory data export requirement schemes if their practices fall within the scope of one exemption but outside the scope of another. For example, for health care or medical device companies that need to transfer customers' biometrics or health care data overseas for the performance of contracts (*e.g.*, the manufacturing of customized medical devices or other healthcare products), it is unclear whether they could rely on the first exemption, given that the data they export would likely be considered "sensitive personal information," which does not seem to fall within the scope of any exemptions under the Draft Provisions. (See the "Heightened Security Assessment Threshold" section below for further discussion on "sensitive personal information").

Accordingly, companies that operate in industries that fall outside of the scope of, or intend to export data that is not expressly covered by, any of the exemptions in the finalized provisions may want to seek clarification from the CAC regarding which particular export requirement schemes they are subject to.

Notably, the Draft Provisions do not alter or otherwise carve out any exceptions to the existing prohibition on exporting data (regardless of whether initially collected in the PRC) to any foreign judicial or law enforcement agency without prior approval by regulators. Thus, companies that need to export data for either purpose should continue to seek approval from the relevant PRC authorities.

### Heightened Security Assessment Threshold

The Draft Provisions provide that only companies that *expect* to export over one million individuals' personal information within the following calendar year need to undergo the Security Assessment, and those that do not exceed this threshold may utilize the less-burdensome Certification procedure or Standard Contract. This forward-looking standard contrasts with the current regulations, which subject companies to the Security Assessment if their practices in the *prior* calendar year satisfied the minimum data transfer threshold.

Notably, the Draft Provisions do not address whether any of the exemptions apply to "sensitive personal information," which is regarded under Chinese law as an individual's biometrics, religious beliefs, health data, financial metrics and travel records, as well as information regarding children under the age of 14. As such, companies that expect to export "sensitive personal information" may seek further guidance from the relevant PRC authorities as to what data transfer mechanisms they are subject.

### "Important Data" Clarification

Under the current regulatory regime, companies are automatically required to complete a Security Assessment if they transfer outside of the PRC any "Important Data," which is broadly defined to

# China Intends To Ease Controls Over Cross-Border Data Transfers

include "data that, once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and safety, and so forth."

"Important Data" is subject to more stringent protection requirements than ordinary data and the lack of certainty about what information falls within this definition has fostered a number of compliance challenges for companies. The CAC endeavoured to remove this ambiguity by clarifying in the Draft Provisions that data processors would not need to treat data as "Important Data" unless specifically categorized as such by the Chinese government through notification or an announcement. This means that companies may presume that they are not processing "Important Data" (and therefore is not obligated to complete a Security Assessment for exporting such data), unless informed otherwise by regulators or a public notice has been issued specifying that the type of data in their possession constitutes "Important Data."

Notably, the Draft Provisions do not affect the existing prohibition on exporting personal information or "Important Data" by critical information infrastructure operators (CIIOs) and government agencies without appropriate approval. See to our November 3, 2021, article "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies" for additional details on CIIOs.

### Free Trade Zones

By allowing free trade zones to determine what types of cross-border data transfers are subject to the mandatory data export procedures, the Draft Provisions would transfer primary administrative responsibilities in certain instances from the CAC to more investment-friendly bodies that may establish even further relaxed cross-border data transfer requirements.

The PRC's Ministry of Commerce designated a pilot set of over 21 free trade zones in various provinces and, with the approval of the relevant provincial CAC, each such zone is authorized to formulate its own list of data that needs to go through different data exportation procedures (Negative Data List), and any future data export activities not covered in that Negative Data List would no longer be subject to the otherwise mandatory Security Assessment, Certification, or Standard Contract.

Companies that do business within any free trade zone should heed the specific data transfer requirements that apply to that zone, particularly given the potential for future "competitions" among free trade zones to attract businesses within their region.

## Conclusion

The Draft Provisions in their current form would significantly ease cross-border data transfer compliance hurdles for companies that do not operate in data-heavy industries, are not CIIOs, and export fewer than one million individuals' data. Although companies may still need to carry out a privacy impact assessment and also obtain data subjects' consent before exporting their personal information, the introduction of the Draft Provisions would undoubtedly improve the PRC's business environment in favor of foreign investors.

## Contacts


**Ken D. Kumayama**
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

**Steve Kwok**
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

**William Ridgway**
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

**David A. Simon**
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

**Siyu Zhang**
Asia Pacific Counsel / Hong Kong
852.3740.4816
siyu.zhang@skadden.com

**Loren C. Shokes**
Associate / New York
212.735.2376
loren.shokes@skadden.com