KIRKLAND & ELLIS

Kirkland Alert

China's Grace Period for Complying with Cross-Border Data Transfer Requirements Has Ended: What Comes Next?

06 March 2023

On March 1, 2023, China's six-month grace period allowing companies to achieve compliance with the security assessment requirements outlined in the Personal Information Protection Law ("PIPL") and the implementing Measures on Data Cross-Border Transfer Security Assessment ("Measures") expired. Thus far, only two companies have obtained formal approval from the central Cyberspace Administration Office ("CAC") to transfer data outside of mainland China.

With no indication that the deadline will be extended, what should companies that have not yet received approvals or are still working toward compliance with the PIPL expect?

1. Background on China's Cross-Border Transfer Requirements

The PIPL (which took effect on November 1, 2021) imposed stringent restrictions and requirements on companies' ability to transfer data outside of China. The PIPL requires personal information ("PI") processors[1] transferring PI outside of China to obtain informed consent from data subjects; conduct a PI protection impact assessment; and fulfill one of three additional requirements: (1) **successfully complete a security assessment conducted by the CAC**; (2) obtain certification from a CAC-approved professional institution; or (3) enter into data transfer agreements with all overseas data recipients consistent with the template agreement issued by the CAC.

The PIPL further clarified that a CAC-conducted security assessment was mandatory for: (1) critical information infrastructure operators ("CIIO")[2] seeking to transfer any PI overseas; or (2) network operators (including non-CIIOs) seeking to export PI of

individuals exceeding certain volume thresholds.[3] Further, the Measures (effective on September 1, 2022) extended this security assessment requirement to any company seeking to transfer "important data"[4] outside of China.

The low PI volume thresholds for network operators, coupled with the broad definition of "important data," rendered many multinational companies subject to the mandatory security assessment requirement. However, the Measures provided a six-month grace period, to March 1, 2023, giving data processors additional time to comply with the security assessment requirement.

2. Status of Security Assessment Filings

The number of companies that have filed security assessments in anticipation of this March 1, 2023, deadline is low. The number of reported approvals is even lower.

According to the Beijing CAC, as of February 22, 2023, only 48 companies had officially filed security assessment applications, which list included applications from at least six leading multinational companies. Only two of these applications, however, have been approved by the CAC — one for a joint research project between a Chinese hospital and a Netherlands-based medical center and a separate application from a Chinese state-owned airline. No applications from multinational companies have yet been approved.

Likewise, the Shanghai CAC announced on February 16, 2023, that it had received security assessment applications from 110 companies, spanning the pharmaceutical, retail, vehicle and finance sectors — but the CAC had yet to approve *any* of those applications.

3. Potential Consequences for Failure to Timely File for Security Assessment

In its February 22 announcement, the Beijing CAC urged companies subject to the security assessment requirements to file applications as soon as possible and highlighted the potential consequences for violating the PIPL's requirements, including:

- ***Administrative Penalties***: Under the PIPL, data processors may face (1) fines up to RMB 50 million (approximately USD 7 million), or 5% of the company's most recent annual revenues (it is unclear from the statute whether this figure is calculated based on the prior year's global revenue or only China-based revenue); (2) forfeiture

of illegal gains; (3) suspension of business operations; (4) revocation of business licenses; and (5) fines for individuals with direct responsibility or involvement in the violations of up to RMB 1 million (approximately USD 143,833).
- ***Criminal Penalties*:** As the Beijing CAC emphasized, serious violations of the Measures also could trigger criminal liability.

Companies that fail to meet the March 1, 2023, deadline to submit applications for a security assessment also may be prohibited from engaging in further cross-border data transfer activities until an application is filed, creating the potential for severe business disruption.

What to Expect

Notwithstanding the CAC's current processing backlog, it remains unclear whether the CAC will extend the grace period for security assessment filings beyond March 1, 2023. If a company engages in transferring data outside of Mainland China and has not already taken steps to comply with the PIPL and the implementing Measures, the company should consider:

- Promptly evaluating whether the company is required under the PIPL to submit a security assessment application;
- Working to submit an application if required; and
- For those organizations that do not fall into one of the categories for which a security assessment is required, checking whether the company has nonetheless: (1) obtained certification from a CAC-approved professional institution; or (2) executed data transfer agreements with the company's overseas data recipients that are consistent with the CAC's template provisions.

---

1. "PI processor" refers to any organization or individual that processes PI, such as companies that collect user data for analytical purposes or for online marketing campaigns. ↩

2. "CIIO" refers to operators of important network facilities, information systems, etc. in important industries and fields which, in the event of a cyberattack or other event, could severely damage national security, the economy, people's livelihood, or public interests. Examples include entities in information and telecommunications, energy, transportation, finance, public services and defense technologies sectors. ↩

3. The thresholds include transferring overseas PI for over 1 million persons in total, transferring overseas PI for over 100,000 persons starting in January 1 of the preceding year, or transferring overseas sensitive PI for over 10,000 persons starting in January 1 of the preceding year. ↩

4. “Important data” refers to any data that, if tampered with, destroyed, leaked, or illegally obtained or used, may endanger national security, public interests, or the legitimate rights and interests of an individual or organization. Examples include geographic information above a certain scale; population census data; financial transaction data of key enterprises; human genetic resource information and population health data; video or image data (including human facial information); license plate information; operating data of a vehicle charging network; etc. ↩

Authors

Yue Qiu

Partner / Shanghai

Jodi Wu

Registered Foreign Lawyer (Kirkland & Ellis, Hong Kong) and Partner (Kirkland & Ellis LLP, U.S.) / Hong Kong

Cori A. Lable

Registered Foreign Lawyer (Kirkland & Ellis, Hong Kong) and Partner (Kirkland & Ellis LLP, U.S.) / Hong Kong

Tiana Zhang

Partner / Shanghai

Related Services

Practices

- Government, Regulatory & Internal Investigations

Suggested Reading

- 17 February 2023 Award Chambers Global: The World's Leading Business Lawyers 2023
- 06 February 2023 Press Release Kirkland Advises Greenbriar Equity Group on $3.475 Billion Fundraise for Oversubscribed Sixth Fund
- 13 January 2023 Award Asia-Pacific and Greater China Region’s Leading Lawyers for Business 2023