KIRKLAND ALERT

April 14, 2017

New Draft China Cybersecurity Regulation on Cross-Border Data Transfer

China's much-anticipated new Cybersecurity Law will take effect on June 1, 2017. Of greatest concern to multinational companies is the data localization requirement imposed on Critical Information Infrastructure Operators ("CIIOs"). The Cybersecurity Law provides that CIIOs shall store any personal information and "important data" collected and generated during their operations within the territory of China and that a security assessment must be conducted if such data must be transferred abroad. However, the Cybersecurity Law provides little clarity on the definition of CIIOs, the meaning of "important data," who should conduct the security assessment, and how it should be conducted — and leaves it to the Cyberspace Administration of China ("CAC") to develop additional regulations.

The draft "Measures on the Security Assessment of Providing Personal Information and Important Data Outside of China" provides some clarity on the important open questions but creates even more ambiguity regarding the scope of the Cybersecurity Law.

On 11 April 2017, the CAC issued a draft "Measures on the Security Assessment of Providing Personal Information and Important Data Outside of China" ("Draft Measures") for public comment. The Draft Measures, provides some clarity on the important open questions but creates even more ambiguity regarding the scope of the Cybersecurity Law. Below is a summary of the key issues in the Draft Measures.

1. Who is captured by the Draft Measures?

The Draft Measures expands the scope of the data localization requirement of the Cybersecurity Law beyond CIIOs to:

- *Network operators* — Under the Draft Measures, all network operators (broadly defined as any network owners, administrators, and network service providers) are subject to the data localization requirement (Art. 2).
- *Other Individuals and organizations* — the Draft Measures include a provision (Art. 16) suggesting that all individuals and entities might be subject to similar security assessment requirements when migrating personal information and other important data outside China.

2. What information is subject to the data localization restrictions?

- *Personal information*
    - The Draft Measures, like other Chinese laws and regulations, defines "personal information" as any information when used independently or in combination with other information, may identify a natural person's identity (Art. 17).
    - Before transferring personal information abroad, network operators must obtain consent for the transfer from the personal information owners *and* inform them of the purpose, scope, content of the export, identity of the recipient, and the country or region where the recipient is located. For underage

information owners, permission of their guardians must be obtained (Art. 4).

- *Important data*
    - The Draft Measures defines "important data" as data closely related to national security, economic development, and social and public interests (Art. 17). Although the definition remains vague, it suggests that day-to-day business information will be unlikely to be included in the scope of "important data" unless the data concerns national security, economic development, and social and public interests.

The Draft Measures suggests that day-to-day business information will be unlikely to be included in the scope of "important data" unless the data concerns national security, economic development, and social and public interests.

3. What security assessment procedures shall be followed?

- *Data prohibited from being transferred outside China*
    - Personal information without the information owner's consent;
    - Data that might impact national security and jeopardize public interest; and
    - Other data which government agencies such as CAC, PSB and national security bureaus do not allow to be exported (Art. 11) (e.g., state secrets, population health information, etc.)
- *Data that can be exported but requires a security assessment to be conducted by government agencies*
    - The following data may be exported, but must first be subject to a "security assessment" by the relevant government agency regulating the company's industry:
        - The personal information of more than 500,000 people at one time, or cumulatively;
        - Information that surpasses 1000 GB in size;
        - Information concerning nuclear infrastructure, chemicals and biology, population health, and data relating to large-scale engineering and construction activities, ocean environment and sensitive geographical information;
        - Cybersecurity information that includes system vulnerabilities and security protections of CIIOs;
        - The personal information and important data of CIIOs; and
        - Other information identified by government agencies (Art. 9)
    - The measures of "security assessment" remain unclear. At this point, it does not appear on its face to include a review of the data intended to be exported.
    - Examples of regulating government agencies responsible for conducting a security assessment may include China Banking Regulatory Commission, China Securities Regulatory Commission, and China Insurance Regulatory Commission. When the industry regulation authority is not clear, the CAC will conduct the security assessment (Art. 9). The government agencies shall

complete the security assessment within 60 working days (Art. 10).

- *Data that can be exported but requires companies to conduct a self-directed security assessment*
    - Network operators must conduct regular security assessments on data to be migrated outside China(Art. 7).
    - The key areas for assessment might include the necessity of providing such data abroad, and the potential risks generated for the national security, the public interest, and legal rights of individuals (Art. 8).
- *Annual Assessment and Reassessment*
    - All network providers must conduct at least one security assessment per year and report the assessment results to the relevant government agency in an industry (Art. 12).
    - Network operators must also promptly re-conduct a security assessment when the recipient of the data changes; the purpose, scope, quantity or category of the data greatly changes; or the recipient of the data or the data provided abroad experiences a significant security incident (Art. 12).

All network providers must conduct at least one security assessment per year and report the assessment results to the relevant government agency in an industry.

4. **What is the effective date of the final Measures?** Because the Cybersecurity Law will take effect on June 1, 2017, we expect the final Measures, as a supplement to the law, to be promulgated before or closely after June 1, 2017.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Tiana Zhang
Kirkland & Ellis International LLP
11th Floor, HSBC Building, Shanghai IFC
8 Century Avenue, Pudong New District
200120 Shanghai
www.kirkland.com/tzhang
+8621 3857 6305

Jodi Wu
Kirkland & Ellis International LLP
11th Floor, HSBC Building, Shanghai IFC
8 Century Avenue, Pudong New District
200120 Shanghai
www.kirkland.com/jwu
+8621 3587 6337

Frank Jeng
Kirkland & Ellis
26th Floor, Gloucester Tower
The Landmark
15 Queen's Road Central
Hong Kong
www.kirkland.com/fjeng
+8621 3761 3532

Yue Qiu
Kirkland & Ellis International LLP
11th Floor, HSBC Building, Shanghai IFC
8 Century Avenue, Pudong New District
200120 Shanghai
www.kirkland.com/yqiu
+8621 3857 6325