KIRKLAND & ELLIS

Kirkland Alert

Newly Released Draft Measures on Data Security Management Strengthen China's Data Protection Framework

10 July 2019

On May 28, 2019, China's central cybersecurity authority, the Cyberspace Administration of China, released a draft of its implementing Measures on Data Security Management (the "Draft Measures") for public comment. The Draft Measures are intended to provide more detailed guidance on how to comply with China's Cybersecurity Law, which was originally enacted in June 2017. Companies doing business in China should be aware of the proposed updates and prepare for the formal adoption of this important legislation in China's data protection framework.

Key elements of the Draft Measures include the following:

- **Definition of "Important Data"**

  China's Cybersecurity Law imposes data localization requirements on critical information infrastructure operators ("CIIOs"), a subset of network operators, to store "important data" collected and generated in their China operation within the territory of China and conduct security assessments before transferring "important data" overseas. The Cybersecurity Law also requires network operators to encrypt and create back-up copies of "important data." "Important data" is broadly defined as data that is closely related to national security, economic development or public interest, a definition that provides little helpful guidance. The Draft Measures clarify that the definition of "important data" does not include production, operational and internal administrative data of enterprises, or personal information (Article 38). The Draft Measures also provide additional examples of "important data," including non-public government information and significant volumes of data related to population, genetics and health care, geographic, and/or mineral resources.

This clarification appears to remove a significant amount of day-to-day operational information from the definition of "important data." However, it remains unclear whether information provided to companies by government entities or state-owned enterprises, whether pursuant to contracts or in other business situations, might still be considered "important data" under the law.

- **Application of Cross-Border Transfer Limitations to Network Operators**

  Perhaps most significant, the Draft Measures require **all** network operators, not just CIIOs, to both: (1) conduct a risk assessment before transferring "important data" outside of China; and (2) seek approval from industry regulatory authorities or provincial cyberspace administrations (if an industry regulatory authority cannot be identified) prior to transferring "important data" outside of China (Article 28).

  The Draft Measures also expand the risk assessment requirement and regulatory approval requirement to include any network operator seeking to publish, share or trade "important data" **domestically** within China. This is a significant increase in the scope of guidelines set out in the original text of the Cybersecurity Law, and one that will likely have a significant impact on companies operating within China (even with the narrowed definition of "important data").

- **New Reporting Requirement for Collection of Sensitive Personal Information and "Important Data"**

  The Draft Measures require network operators — defined under the Cybersecurity Law to include virtually any company with business operations and information technology in China — that collect sensitive personal information or "important data" as part of their operations to report their collection activities to the local cyberspace administration (Article 15). Any such report must specify the guidelines the network operator applies to its data collection and use, including the purposes, volume, methods, scope, types and retention period. Nevertheless, the Draft Measures do not require a network operator to provide copies of the underlying data to authorities. Importantly, however, the Draft Measures do not specify how (or how frequently) these reports should be made to authorities.

  Because the definition of "sensitive personal information" is broad and potentially covers information such as ID card numbers, cellphone numbers and location information, many companies operating in China will likely be subject to the new reporting requirement (although the requirement's contours remain unclear).

- **Required Designation of Data Protection Officer**

  The Draft Measures also require network operators that collect sensitive personal information or "important data" to appoint a Data Protection Officer ("DPO") with relevant experience and knowledge to manage data security (Article 17). The key responsibilities of a DPO include devising and implementing data protection plans, conducting a data security risk assessment and remediating identified gaps, reporting handling of incidents to relevant authorities and handling user complaints (Article 18). Again, due to the broad definition of "sensitive personal information" and "important data," most companies operating in China will likely need to appoint a DPO in China once these Measures come into effect.

- **Expanded Personal Information Collection Restrictions**

  The Draft Measures require network operators to include rules on the collection and use of personal information in their privacy policies and to provide copies of those policies to users (Article 7). The Draft Measures also clarify that obtaining consent in a misleading manner is insufficient under the law. Further, the Draft Measures forbid network operators from refusing to provide their core service to a user after a user has provided personal information needed to operate the core service, or to discriminate among different users based on their consent to provide personal information (Article 11). Finally, the Draft Measures require network operators to obtain consent from parents or guardians prior to the collection of personal information of minors under the age of 14 (Article 12).

- **Broadened Scope of Responsibility for Personal Information Protection**

  The Draft Measures also clarify that a network operator is responsible for protecting personal information that it obtains from "other channels," not just information it directly collects (Article 14). This requirement, which broadens the original scope provided under the Cybersecurity Law, may subject third parties that process personal information for other entities to heightened data protection obligations.

- **Explicit Data Protection Obligations in Corporate Transactions**

  The Draft Measures explicitly provide that successor companies assume data protection obligations and responsibilities of network operators following mergers and acquisitions, restructurings and bankruptcy proceedings (Article 31). This added provision suggests that companies considering such transactions in

China should undertake cybersecurity and data protection compliance as part of any due diligence process.

Recommendations

In anticipation of the forthcoming enactment of the Draft Measures and existing cybersecurity and data protection legislation, companies doing business in China should consider the following best practices:

- Conduct a risk assessment to understand their current data collection, use and transfer practices to identify potential compliance gaps and necessary enhancements;
- Review and update privacy policies to comply with the heightened disclosure requirements;
- Consider appointing a DPO if the company collects personal information or "important data" in China; and
- Continue to monitor the development of relevant laws, regulations and national standards to ensure an accurate and up-to-date understanding of applicable data protection obligations.

Authors

Tiana Zhang

Partner / Shanghai

Cori A. Lable

Partner / Hong Kong

Jodi Wu

Partner / Shanghai

Richard Sharpe

Partner / Hong Kong

Yue Qiu

Associate / Shanghai

Related Services

Practices

- Litigation
- Government, Regulatory & Internal Investigations

Suggested Reading

- 08 July 2019 Article INSIGHT: U.S. Trade Secret Prosecutions—Should Chinese Companies be Worried?
- 03 July 2019 Kirkland Alert China to Release an “Unreliable Entity List”
- July-August 2019 Article Minimizing Your Company's Exposure to a Ransomware Attack