AmCham China
中 国 美 国 商 会

INSIGHTS

Navigating the Chinese Cybersecurity Law

Ambiguity remains a common concern

"Managing China's Cybersecurity Law Updates" – May 18, 2018

HIGHLIGHTS AND KEY TAKEAWAYS

- Cyber-sovereignty—a government's desire to regulate the internet within one's borders—remains the overarching theme as Chinese Cybersecurity Law (CSL) guidelines continue to be released.
- Ambiguity remains the top concern among event attendees. Key terms in the CSL, including "personal data" and "critical information infrastructure" are not clearly defined, and members are concerned that regulation of the information and communications technology industry might be decentralized and inconsistently enforced.

Executive Summary

Although China has now established a relatively comprehensive regulatory regime for cybersecurity following passage of the CSL on November 7, 2016, many foreign companies in China still find it challenging to comply with the CSL and its evolving implementation guidelines.

What are the updates?

- The Personal Information Security Specification (个人信息安全规范) entered effect on May 1, 2018.
    - The Specification is divided into two categories: personal information (e.g., location tracking) and sensitive personal information (e.g., individual biometrics).
    - Exceptions to the consent requirements, including scenarios related to national security and other public interests, have been further clarified.
    - The Specification does not have the force of law, but it could become mandatory when it is referred to in other laws and regulations. This is one example of uncertainty regarding implementation that is of concern.
- CSL Articles 31 to 39 (关键信息基础设施的运行安全, "Safety Rules on Critical Information Infrastructures (CII)")
    - It is unclear whether *all* businesses classified as CII will be subject to the same level of scrutiny.

  - "Critical Industries" (重要行业和领域, see Article 31) classified as CII include telecommunications, energy, transportation, information services and finance, but the list is not yet comprehensive.
  - Article 35 specifically signals further governmental supervision on Information Technology procurements that must pass some national security inspections; however, details remain opaque.
- Articles 21 to Article 30 (协助政府机构, "Governmental Assistance and Reporting"):
  - "Network operators" must report any data-related emergencies including breaches, losses and destructions to relevant authorities immediately, but neither the timeline or the name of the authorities is clear.
  - Network operators must also assist legal authorities by providing technical support and assistance. The scope of such assistance remains unclear.
- Article 37 (数据本地化, "Data Localization")
  - Mandates all network operators in critical industries to store critical and personal information within the territory of China.
  - Data security assessments determining whether cross-border data is necessary are composed of two factors: "lawful purpose" and "low security risk."
  - The new requirements on data localization will result in sizable compliance adjustments for foreign companies in China.
  - It remains unclear which companies will be required to undergo these security assessments.

What can foreign businesses do to cope with the upcoming changes?

- Actively involve legal and compliance teams in daily business operations.
- Prepare contingency plans for potential data breaches and other data-related incidents and conduct privacy impact assessments periodically. Adjust scenarios accordingly as the implementation guidelines evolve.
- Hold internal compliance trainings for both employees and third-party business associates.
- Review contractual provisions for agreements with business associates.

If you have questions about the event and or would like to join AmCham China's Information Communications and Technology Forum or Compliance Committee, please contact Evan Schmitt.

For inquiries on Insights, please contact Chloe Ma.