China Releases Regulations on Network Data Security Management

December 12, 2024 Liza Mark

PRACTICES Asia, China, International

On Sept. 24, 2024, China's State Council released the "Regulations on Network Data Security Management" (《网络数据安全管理条例》) (the "**Regulations**"), to take effect on Jan. 1, 2025. The Regulations introduce specific controls for network data processors, focusing on issues concerning personal information (the "**PI**"), important data, and cross-border data transfers. On the legislative hierarchy, the Regulations provide detailed guidance on the implementation of China's trio of laws governing data protection, i.e.: Cybersecurity Law (《网络安全法》) (CSL), Data Security Law (《数据安全法》) (DSL) and Personal Information Protection Law (《个人信息保护法》) (PIPL) (collectively, the "**Data Laws**"), and are superior to the rules issued by the Cyberspace Administration of China (CAC) in relation to specific regulatory matters. The Regulations affect all businesses that process electronic data and are relevant to businesses of all sizes, especially their internal data processing systems.

Here is a summary of the highlights of the Regulations:

1. **TAKEAWAYS**

The Regulations were finalized after more than three years of lengthy rule preparation and consultation by China's State Council. They address key issues previously left open by China's set of Data Laws, especially with respect to the classification of "Important Data" and relating data protection measures. The Regulations suggest that reporting of data incidents, data protection agreements, record-keeping and compliance assessments/reporting will likely become the new enforcement focus of the CAC.

As such, businesses are advised to conduct at least the following compliance checks before the Regulations take formal effect in 2025:

- Revise and update privacy policies, preferably with a Chinese addendum to reflect the most up-to-date obligations under the PIPL.
- Online platform operators need to constantly monitor in-platform data processing activities to ensure that data and algorithms on their platforms allow for equal access by users and are not abused to discriminate.
- Businesses that process PI and/or Important Data should conduct a comprehensive review of data processing activities and clarify their subject.
- Businesses that have cross-border data transfer necessities should evaluate if their situations would fall within the now-expanded permissible data export scenarios, which exempt the otherwise-required mechanisms of security assessment, certification or the standard contract.
- Businesses should use tools, including risk assessments, compliance audits and annual reporting to fulfil their security management responsibilities as well as to improve their own network data security management capabilities.

Read the full article here.