Revised draft cyber security law may significantly impact multinationals in China

August 30, 2016

China's government released a second draft of its cyber security law on 5 July 2016. Once adopted, this law will likely have a significant impact on all business sectors in China. Compared to the first draft, which was previously highlighted in In context, the new draft contains few adjustments. With this draft available to the public, the adoption of the new law moves one step closer.

We recommend that multinationals active in China closely monitor further legislative developments; specifically, the requirements relating to the storage of data in China and the inspection of certain key network products before they can be sold in China.

Requirement to store data in China

The cyber security law (CSL) requires companies to store certain information within the mainland territory of China. This information may be transferred abroad only if there is a business purpose which requires the transfer and if a security assessment has been conducted.

The "localisation requirement" applies to companies that operate "critical information infrastructures". In the first CSL draft, this term was defined broadly and included a catch-all for networks with a large number of users. In the second CSL draft, the definition of critical information infrastructures operators was omitted. Instead, the State Council has been given the task of clarifying the scope, which effectively gives the government more flexibility.

The information concerned consists of personal information of Chinese citizens and important business data generated during operations in China. The CSL does not specify what is meant by the rather general term "important business data".

After a security assessment, information may be transferred abroad if a specific business purpose requires this. No guidance is given on the manner or form of the security assessment. The first CSL draft explicitly stated that after the security assessment, information could be stored abroad or provided to individuals or organisations abroad. The second CSL draft only states that information can be exported abroad, and it deletes the term "storage". Consequently, the possibility to transfer data out of China seems to have narrowed.

Given the potentially broad application of the localisation requirement, multinational companies should take into account that cross-border transfers of information between Chinese subsidiaries and overseas operations may be restricted and may be subject to a security assessment.

Key network equipment and network security products subject to inspection

Under the CSL, providers of key network equipment and network security products must have their products inspected or certified by a qualified institution before these can be sold in China. At this stage, it is uncertain which types of products will require this certification. The CSL anticipates that those products will be identified in catalogues to be published by the State Network and IT authorities together with the State Council. Companies providing key network equipment and network security products, as well as companies relying on the use of those products in China, will need to take into account that there may be delays before the products can enter the market or that the products may not be sold in China if they have not been approved. Another concern with this requirement is that the standards for review have yet to be developed. In the first draft, other countries commented that the standards to be used should be based on international standards. The second draft makes no reference to international standards.

A review of the first and second CSL drafts seems to show no willingness on the government's part to clarify the terms of the CSL and thus limit the potentially broad implications of the CSL. Even after adoption of the CSL, the scope and applicability of obligations are likely to remain unpredictable. Multinationals with operations in China are advised to closely monitor any developments in relation to the CSL and, more importantly, its implementation by the relevant authorities.