COSMOS
Navigate the Compliance Universe

# Report on Supply Chain Compliance Volume 2, Number 12. June 27, 2019
# Who's responsible for what here? Questions surround updates made to China's Cybersecurity Law

By Sascha Matuszak

In the two years since China's Cybersecurity Law (CSL) has officially been in force, companies doing business in China have adopted a "wait and see" attitude toward a number of provisions in the law. Chinese authorities have made tweaks and changes to the law over the past 18 months, including arguably the most anticipated draft measure, Second Draft Measures on Security Assessment for Export of Personal Information, released on June 13. The Second Draft Measures are open for public consultation until 13 July 2019. An unofficial translation of the draft can be read here.

These measures address the data localization and data transfer provisions of China's Cybersecurity Law, provisions that foreign companies active in China feared could lead to the loss of business secrets to competitors or to the Chinese authorities themselves. The article in question, Article 37, reads as follows:

> Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.

There have been a few key changes to the language that companies should be aware of.

## Key amendments

The draft covers only personal information and does not yet address important or critical data (i.e., business data). The draft also applies the data export requirement to "network operators," which is an expansion of the scope of the original article that applied the requirements to "critical information infrastructure operators." The new draft language of the requirements laid out in Article 37 can be translated as follows:

> Network operators providing those outside the mainland territory with personal information collected by operators inside the mainland territory of the People's Republic of China (hereinafter 'personal information leaving the country') shall conduct security assessments in accordance with these Measures. Where through security assessments it is determined that personal information leaving the country might impact national security or harm the public interest, or that it would be difficult to ensure personal information security, it must not leave the country. Where the state has other provisions on personal information leaving the country, follow those provisions.

An assessment by Michelle Chan and Clarice Yue of Bird & Bird clarifies further:

> The Second Draft Measures however do not appear to expressly impose any data localisation requirement on network operators. It is important to note that businesses operating outside of China (thus not just a 'network operator' in China) will also be caught by the Second Draft Measures. Article 20 of the Second Draft Measures provides that entities operating outside of China but collecting personal information of individuals in China through the Internet (or other means) are required to [go] though their legal representatives in China to comply with the obligations applicable to network operators in China.

Additionally, changes have been made to the security filings that companies must submit before transferring or exporting personal data; the particular questions that a security review must answer; and obligations regarding storing data, as well as annual reports detailing the data being stored, exported or transferred, and the reasons for doing so.

Of particular interest are the requirements for contracts between network operators, data subjects and data recipients. These requirements appear onerous, but are in effect not very different from the same burdens imposed by GDPR regulations governing the interactions between network operators and data subjects. Indeed, previous drafts amending and clarifying aspects of the CSL have discussed consent and the problem of "bundled consent" — China has come to similar conclusions as European regulators: network operators are forbidden from obtaining bundled consent. Some of the contractual requirements are:

- "the contracts must set out the purposes of the export, the types of personal information involved, and the period for which the data will be retained abroad,
- "network operators must notify the data subjects of the export;
- "the data subjects will be named as a third party beneficiary in the relevant contracts and be given the right of recourse against the data recipients and the network operators;
- "the data recipient is not permitted to further transfer the personal information to a third party unless certain conditions are satisfied, including that a consent has been obtained from the data subjects concerned."