MAYER·BROWN
JSM

Legal Update
Mainland China
21 April 2017

China Expands the Scope of the Data Localisation Requirement under its Cybersecurity Law

On 11 April 2017, the Cybersecurity Administration of China (CAC) released the draft Security Assessment Measures for Cross-Border Transfer of Personal Information and Important Data ("Draft Measures"). Draft measures and guidelines relating to the Cybersecurity Law (CSL) which was released in November last year, have been expected for a while. The hope has been that such guidelines and measures would shed light on the more opaque terms in the CSL and offer some clarity on the interpretation of broad definitions and concepts. The Draft Measures address the data localisation requirement but instead of narrowing down the concept, they appear to have further expanded the scope of this requirement, thus creating more uncertainty. The data localisation requirement was originally applicable to critical information infrastructures (CIIs) only. The Draft Measures indicate that it should cover both CIIs and network operators. If adopted, the Draft Measures will impose data localisation requirements on multinational companies (MNCs) which previously believed they were not CIIs thus not subject to these rules. The consultation period for the Draft Measures will end on 11 May, shortly before the 1 June effective date of the CSL.

Article 37 of the CSL requires operators of CIIs to store personal information and important data gathered and produced during their operations in China within the territory of China, and to obtain a security assessment from the authorities if such data is to be provided abroad. Article 2 of the new Draft Measures expands Article 37 by further requiring network operators to comply with the rule:

> *Network operators shall store personal information and important data gathered and produced during operations within the territory of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with these Measures.*

The Draft Measures propose two types of security assessments a network operator shall conduct: a self-assessment and an official security assessment undertaken by the relevant authorities.

The factors to be considered in the self-assessment include:

- necessity of the cross-border data transfer
- the quantity, scope, type, and sensitivity of the personal information to be transferred
- the quantity, scope, type, and sensitivity of the important data to be transferred
- the adequacy of the data protection measures the data recipient is capable of adopting, and the network security environment of the recipient country/region
- the risks of the transferred data being disclosed without authorisation, destroyed, modified, misused, or otherwise compromised
- the likelihood of causing harms to national security, public interest, and an individual's legitimate interest once the data is transferred abroad
- any other important factors

The self-assessment shall be conducted at least once a year and/or upon any important change to a transaction involving a cross-border data transfer, including, for example, any significant change in the purpose, scope, quantity, and type of data being transferred, or upon a serious security breach incurred by the recipient or pertaining to the data being transferred.

In addition to the self-security assessment, network operators shall also obtain an official security assessment from the relevant government authorities

if one of the following circumstances applies:

- the personal information to be transferred concerns more than 500,000 individuals
- the data to be transferred exceeds 1,000 GB
- the data to be transferred is from sectors such as nuclear, biochemical, national defense, military, healthcare, marine engineering, or contains sensitive geographic data
- the data concerns security vulnerabilities and protection of CIIs
- operators of CIIs providing personal information and important data abroad
- any other cross-border transfers that would potentially affect national security and public interest

An official security assessment shall be completed within 60 working days by the relevant government authorities. The results of the official assessment need to be reported to the CAC.

The Draft Measures prohibit the cross-border transfer of personal information and important data in any of the following three scenarios:

- Without the data subject's consent. A business entity shall notify the data subject of the purpose, scope, content, the recipient, and the recipient country/region of the transfer, and obtain the data subject's consent. Cross-border transfer of personal information pertaining minors shall obtain the consent of the minor's legal guardian.
- When the proposed cross-border data transfer may jeopardise national security and public interest, and cause harms to government, economy, science, and national defense.
- When government authorities deem the transfer inappropriate.

The Draft Measures define "provision of data abroad"/"cross-border data transfer" to mean a network operator providing personal information and important data collected and gathered within the territory of China to an organisation, entity, or individual abroad. The phrase "important data" is defined to mean "data closely related to national security, economic development, and public interest." This definition, however, fails to clarify whether data derived from personal information such as meta data, statistical data, and encrypted data which are typically excluded from cross-border transfer regulations in other jurisdictions, falls under the CSL. The exact procedure and scope of the official security assessment is not specified although the factors listed for the self-security assessment may be relevant considerations.

Despite the remaining ambiguities in some key terms, the Draft Measures bring in some recognisable privacy procedures and principles such as user consent as a pre-requisite to cross-border data transfer, and the yardstick of adequacy of the data protection measures of the recipient/recipient country in determining whether or not to approve a cross-border data transfer. MNCs will need to re-evaluate their data localisation obligations under this expanded rule particularly in light the fact that most MNCs would likely be deemed to fall within the definition of network operator, i.e., owners and administrators of networks and network services providers, which has been liberally interpreted by most commentators so far, as covering any operator of services provided over the Internet, short of any on point clarification from the Chinese authorities.

For now, MNC are advised to concentrate their efforts on taking steps to ensure compliance with the security assessment requirements if any cross-border data transfer is to be contemplated. While the Draft Measures are still open for comment, it is unlikely that lobbying efforts will bear much fruit. As far as any preparatory work for compliance is concerned, MNCs may consider adopting a three-step approach: i) first, re-evaluate their current privacy policies and procedures for their China operations to ensure adequate notice has been given to users and proper consent has been obtained with regards to all cross-border data transfers; ii) second, prepare a self-security assessment check list by gathering information regarding the transfers such as the type, quantity, and sensitivity of the data, and the adequacy of data protection measures of the recipient vendor and of the country/region where the recipient resides and iii) third, conduct a global vendor re-assessment and eliminate high-risk vendors (de-coupling) or consolidating others.

Contact Us

For enquiries related to this Legal Update, please contact the following persons or your usual contact at our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Xiaoyan Zhang
Counsel (New York, USA)
T: +852 2843 2209
E: xiaoyan.zhang@mayerbrownjsm.com