ALLEN & OVERY | 朗悦
LANG YUE | 安理国际律师事务所

China consults on security assessments for cross-border transfer of data

November 3, 2021

On October 29, 2021, the Cyberspace Administration of China (**CAC**) issued draft **Measures on Security Assessments for the Cross-border Transfer of Data** (a consultation draft for public comment) (**Draft Measures**). These are designed to address the situation where there is a need for the transfer of data outside Mainland China primarily in connection with day-to-day business activities. Notably, the measures do not directly address the issue of cross-border data export in connection with overseas proceedings or investigations, or with the provisions in the PRC Data Security Law (**DSL**) (Article 36) and Personal Information Protection Law (**PIPL**) (Article 41), which has been getting a lot of attention from commentators.

The Draft Measures should be read in conjunction with the PRC Cybersecurity Law (**CSL**), the DSL and the PIPL. Terms used in these laws, notably the concepts of Important Data and Personal Information, are also used in the Draft Measures. The consultation period will last until November 28, 2021.

The Draft Measures outline the approach the CAC will take to the security assessments and protocols that must be put in place before data collected and generated through operations in Mainland China may be transferred outside Mainland China. This note summarizes the key provisions of the Draft Measures and proposes a number of potential clarifications. Before this, by way of reminder, we set out the definitions, or lack thereof, of two key terms used in the Draft Measures: Important Data and Personal Information.

Important Data and Personal Information

Important Data

There is presently no general definition of the term 'Important Data' in Chinese law, although it would appear to be data which, while viewed as sensitive, does not technically fall under the PRC state secrets regime. The concept was first signaled in Articles 21 and 36 of the CSL in 2017. Earlier this year, Article 21 of the DSL provided some guidance as to how the term would be defined and explained that relevant government departments would be working to formulate relevant catalogs for Important Data under a national data security coordination mechanism. In other words, the term may be defined on a sector-by-sector basis. One example of this approach is the *Several Provisions on Automotive Data Security Management (for Trial Implementation)* (August 2021) recently promulgated by, among others, the Ministry of Transport as the primary government agent supervising the automotive industry (**Automotive Data Provisions**).

Under Article 3 of the Automotive Data Provisions, Important Data is "data that may endanger national security, the public interest or the legitimate rights and interests of individuals or organizations once they are tampered with, damaged, disclosed, illegally obtained or illegally used," including: (a) data relating to important sensitive areas such as military administrative zones, entities of science, technology and industry for national defense, and Party and government organs at the county level or above, including geographic information, passenger flow, vehicle flow etc.; (b) data reflecting economic operations such as vehicle flow, logistics, etc.; (c) the automobile charging network's operational data; (d) outside-the-vehicles video and image data that contains facial recognition, license plate information, etc.; (e) personal information of more than 100,000 data subjects; and (f) other data that may endanger national security, the public interest or the legitimate rights and interests of individuals or organizations as determined by the CAC and the authorities for development and reform, industry and information technology, and public security and transport, etc., under the State Council.

Similarly, some other forms of the definition of important data could be found, for example, in the consultation draft issued by the Ministry of Industry and Information and Technology on data security and an unofficial draft Identification Guide to Important Data. It is clear that the concept of important data is likely to continue evolving.

Personal Information

Unlike the situation with the definition of Important Data, the definition of the term 'Personal Information' is more straightforward. For the purposes of the Draft Measures, Personal Information is as defined in Article 4 of the PIPL: "a variety of information related to an identified or identifiable natural person that is recorded electronically or otherwise, excluding anonymized information." Raw human resources data or customer data is likely to be considered Personal Information for the purposes of the law.

With these definitions in mind, we now turn to an examination of the Draft Measures.

Self-assessment

Data processors must carry out self-assessment before transferring data outside Mainland China. Article 5 sets out the key aspects of such self-assessment. A self-assessment report must also form part of the application documents to the CAC for a security assessment (Article 6). It would be helpful if CAC could clarify whether the Article 5 self-assessment applies to export of data which is neither Important Data nor Personal Data in the context of Article 40 of the PIPL (collectively, **General Data**), and, if yes, the minimum retention period of the self-assessment report of General Data, the legal penalty for violation in respect of General Data, etc.

Scenarios in which a CAC security assessment is required

The Draft Measures (Article 4) specify that a CAC security assessment must take place in any of the following scenarios:

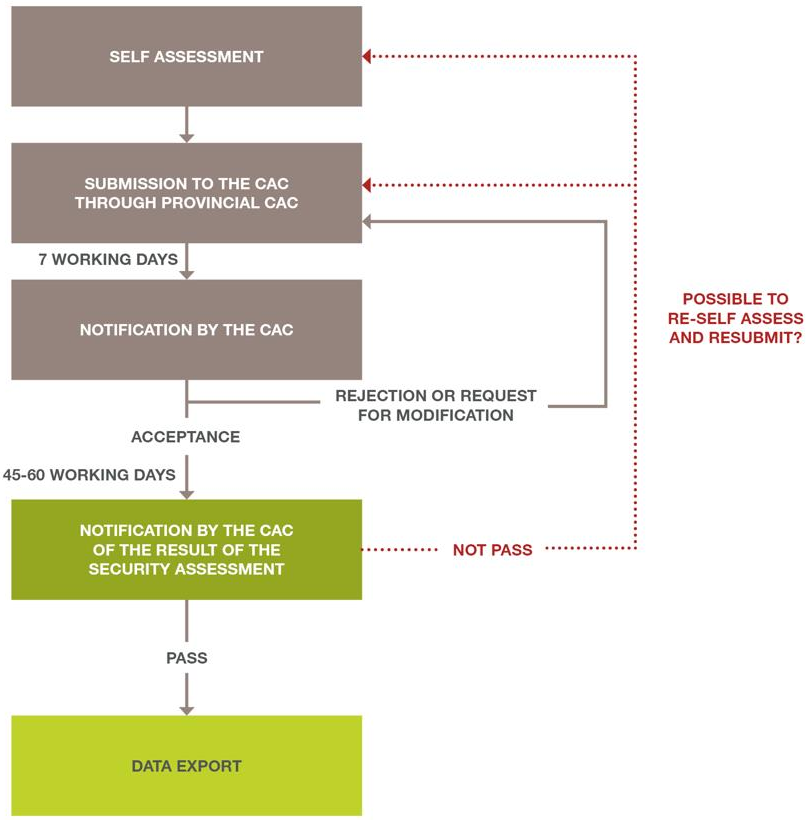
i. where there is a transfer of Personal Information or Important Data collected and produced by a Critical Information Infrastructure Operator (CIIO);
ii. where the data to be exported contains Important Data;
iii. where the personal information processor exporting personal data processes the Personal Information of one million data subjects or more;
iv. where the cumulative volume of Personal Information transferred reaches the volume of 100,000 data subjects;
v. where the cumulative volume of sensitive Personal Information reaches the threshold of 10,000 data subjects; and
vi. other situations determined by the CAC.

As can be seen from the list above, the CAC adopts a hybrid of qualitative and quantitative approaches to define scenarios that require security assessment. There is notably no safe harbor for intra-group data transfer. If a China subsidiary of an MNC needs to transmit data to its headquarters in the U.S. and this falls within any of the above scenarios, it will need to pass the CAC security assessment.

There are a number of points that may need clarification here. The drafting of scenario (iii) suggests that, as long as the personal information processor processes data above the threshold, it will need to pass the CAC security assessment even if it only exports the personal information of a single data subject. One would question whether this is truly the intention of the drafters or whether this is commercially practicable. Scenarios (iv) and (v) both refer to "cumulative volume." It may be helpful to clarify whether such accumulation only starts from the effective date of the law to avoid any confusion (to include historical transfers).

The process for a CAC security assessment

The Draft Measures set out the steps involved in a CAC security assessment. Please refer to the flowchart below.



As anticipated, a CAC security assessment will generally be valid for two years unless certain changes take place and trigger a re-assessment. Among those triggers, some may need clarification. For example, what constitutes a "change in the actual control" of the overseas data recipient "that may affect the security of the exported data"? It is clear that certain notification processes must be built into the agreement with the overseas data recipient to ensure that the data exporter is aware of such a change in a timely manner, in particular when publicly available information is limited. This leads to our next topic: the agreement to be concluded between the data exporter and the overseas data recipient in respect of the data export (**DTA**).

Requirements of a DTA

A DTA is a key document for both the self-assessment and the CAC security assessment. To assess whether the DTA has sufficiently covered the responsibilities and obligations involved in data security is a key aspect of the security assessment.

Article 9 of the Draft Measures sets out various requirements for the DTA which must contain at least the following：

- the purpose, method and scope of data export, the purpose and method etc of data processing by overseas data recipients;
- the location and duration of data storage overseas, and the processing measures after the expiry of the data storage period, the fulfillment of the agreed purpose of the data processing or the termination of the DTA;
- binding clauses restricting the further transfer of data by overseas data recipients to other organizations and individuals;
- security measures that the overseas data recipients should take if there is a substantial change of control [of the overseas data recipients] or [a substantial change in] their business scope, or in the legal landscape of the country or jurisdiction where the data is located, which makes it difficult to ensure data security;
- responsibilities for any breach of data security protection obligations and binding and enforceable dispute resolution clauses; and
- in the event of data leakage and other data security risks, emergency responses should be properly carried out and unobstructed channels for individuals to safeguard their data subject rights should be made available.

One fundamental question we have in respect of the Draft Measures is to what extent the provisions relating to self-assessment or the DTA apply to scenarios outside the scope of Article 4. Are the self-assessment and the DTA only envisaged as part and parcel of the security assessment? The scope set out in Article 2 would suggest the answer is yes but it is not entirely clear.

Suggested action items

- Businesses should conduct a mapping exercise to ascertain the nature of data to be transferred and the amount of data subject to overseas transfer. This would assist a business in assessing whether a CAC security assessment may be needed for its data export and in considering whether alternatives exist to avoid such an assessment.
- If a CAC security assessment is likely to be required and cannot be avoided, a self-assessment should be conducted with counsel's assistance to ensure that it meets the requirements of the Draft Measures.
- At the same time, businesses should start reviewing their own DTAs for the purpose of identifying whether they are legally compliant.
- The data export protocol should be set up or updated as required by the new laws.

Key Contacts in China

Allen & Overy

Victor Ho
Registered Foreign Lawyer, Hong Kong
Managing partner of A&O Beijing and Shanghai
Tel +852 2974 7288
victor.ho@allenovery.com

Jane Jiang
Partner, Shanghai
Tel +86 21 2036 7018
jane.jiang@allenovery.com

Eugene Chen
Registered Foreign Lawyer, Hong Kong
Tel +86 852 2974 7248
eugene.chen@allenovery.com

Susana Ng
Of Counsel, Hong Kong
Tel +852 2974 7015
susana.ng@allenovery.com

Richard Qiang
Counsel, Beijing
Tel +86 10 6535 4306
richard.qiang@allenovery.com

Richard Wagner
Registered Foreign Lawyer, Hong Kong
Tel +852 2974 6907
richard.wagner@allenovery.com

Lang Yue

Melody Wang
Partner – Lang Yue
Tel +86 21 2067 6988
melody.wang@allenoveryly.com

Ran Chen
Litigation Counsel – Lang Yue
Tel +86 10 8524 6100
ran.chen@allenoveryly.com

Allen & Overy Lang Yue (FTZ) Joint Operation Office

Room 1501-1510, 15F Phase II IFC Shanghai, 8 Century Avenue, Pudong, Shanghai China

Allen & Overy LLP, Shanghai office: Tel: +86 21 2036 7000 FAX: +86 21 2036 7100

Shanghai Lang Yue Law Firm: Tel: +86 21 2067 6888 FAX: +86 21 2067 6999

Allen & Overy Lang Yue (FTZ) Joint Operation Office is a joint operation in the China (Shanghai) Pilot Free Trade Zone between Allen & Overy LLP and Shanghai Lang Yue Law Firm established after approval by the Shanghai Bureau of Justice.

Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales. Allen & Overy LLP is a multi-jurisdictional legal practice with lawyers admitted to practice in a variety of jurisdictions.

The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of members' names and of the non-members who are designated as partners is open to inspection at its registered office, One Bishops Square, London E1 6AD, United Kingdom and at the above address. Services in relation to the laws of the People's Republic of China are provided through Allen & Overy LLP's joint operation with Shanghai Lang Yue Law Firm.

Shanghai Lang Yue Law Firm is a general partnership formed under the laws of the People's Republic of China with law firm licence number 23101201410592645 whose registered office is at Room 1514 – 1516, 15F, Phase II, IFC, 8 Century Avenue, Shanghai 200120. It was established after approval by the Shanghai Bureau of Justice. A list of the partners and lawyers of Shanghai Lang Yue Law Firm is open to inspection at its registered office or via the Shanghai Bar Association.