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

CAC publishes draft regulations for network data security management

29 November 2021

On 14 November 2021, the Cyberspace Administration of China (**CAC**) published a consultation draft of the *Regulations on Network Data Security Management* (**Network Data Security Regulations**) for public comment. The subject matter of the draft appears on the 2021 legislative plan for the State Council and thus, while the CAC has published the draft, the promulgating authority may ultimately be the State Council.

The draft seeks to provide more detail and to address certain provisions set out in the *PRC Cybersecurity Law* (**CSL**), the *PRC Data Security Law* (**DSL**) and the *PRC Personal Information Protection Law* (**PIPL**). The consultation period is open until 13 December 2021. This note summarises a few key provisions of the draft Network Data Security Regulations that are most relevant to MNCs and proposes a number of potential clarifications.

More detailed definition of Important Data

Important Data and Personal Information look to be the key data types that would be further elaborated under the Network Data Security Regulations. The draft provides for two separate chapters concerning the processing of Personal Information and Important Data, respectively.

Unlike the straightforward definition of Personal Information in the PIPL, the term "Important Data" has not been given a general definition in earlier laws. The draft Network Data Security Regulations provide a welcome general definition. Important Data is defined in the draft as "data that may endanger national security and public interest if tampered with, destroyed, leaked, or illegally obtained or illegally used". A non-exhaustive list of Important Data is also set out in the draft as follows:

a) Undisclosed government affairs data, employment secrets, intelligence data and law enforcement and judicial data.
b) Export control data, core technologies, design plans, production processes and other related data affecting export control items, and scientific and technological achievements data in fields such as cryptography, biology, electronic information and artificial intelligence that have a direct impact on national security and economic competitiveness.
c) National economic operations data, important industry business data, statistical data, etc. that need to be protected or controlled as expressly stipulated by national laws, administrative regulations and departmental rules.
d) Safe production and operation data and key system components and equipment supply chain data in key industries and fields such as industry, telecommunications, energy, transportation, water conservancy, finance, the defence technology industry, customs, taxation, etc.
e) Basic national data on population, health, natural resources and the environment, such as genes, geography, minerals, meteorology, etc., that meet the scale or accuracy standards stipulated by the relevant national departments.
f) The construction, operations and security data of national basic infrastructures and critical information infrastructures, and the geographic locations, security conditions and other data of important sensitive areas such as national defence facilities, military management areas, national defence scientific research and production units and others.
g) Other data that may affect the security of the country's politics, land, military, economy, culture, society, science and technology, ecology, resources, nuclear facilities, overseas interests, biology, space, polar regions, and deep seas.

As we stated in our previous note (click **here**), it is expected, under Article 21 of the DSL, that the definition of Important Data will be further elaborated on a sector-by-sector basis.

Provisions Addressing the Extraterritorial Scope of China's Data Law Regime

The draft Network Data Security Regulations also address exterritorial effects under the PIPL and the DSL. Article 2 provides that the Network Data Security Regulations apply to, in addition to all data processing that takes place in China, those processing activities carried out outside the territory of the PRC affecting the "data of individuals and organisations located in China" in certain circumstances, as enumerated below:

a) for the purpose of providing products or services into the territory of the PRC;
b) for analysing or evaluating the behaviour of persons or organisations in the territory of the PRC;
c) involving the processing of Important Data in the territory of the PRC; or
d) other circumstances stipulated by laws and administrative regulations.

In comparison to the PIPL, extraterritorial effect extends to the data of "organisations located in China" (**Organisation Data**) in addition to the data of individuals located in China. Unlike the DSL, the extraterritorial effect on Organisation Data is no longer limited to cases where the processing activities harm the interests of China or its citizens or organisations. Instead, the Network Data Security Regulations would apply to the offshore processing of Organisation Data regardless of whether such processing harms China's interests or not.

Expanded regulatory requirements on cross-border data transfer?

Conditions to cross-border data transfer

Article 35 of the draft Network Security Regulations provides that one of the following conditions must be met before a data processor may transfer *any data* overseas (**General Conditions**):

a) a security assessment organised by the state cyberspace authority has been passed; or
b) both the data processor and the data recipient have obtained personal information protection certification from a professional institution recognised by the state cyberspace authority; or
c) a contract (ie a Data Transfer Agreement) has been entered into with the overseas data recipient in accordance with regulations promulgated by the state cyberspace authority on standard contracts; or
d) other requirements under laws, administrative regulations or the rules of the state cyberspace authority have been satisfied.

These conditions are similar to those set out under Article 38 of the PIPL in respect of Personal Information (**PI Conditions**) but effectively expand the application of such conditions to "any data", including data that is not Personal Information. There is no exception based on the volume or the nature of the data. It is expected that this provision, if it were to come into force as presently drafted, could significantly add to the burden of multinational companies' cross-border data activities involving China.

One of the differences between the General Conditions and the PI Conditions is that General Condition (c) above only requires the relevant contract to be "in accordance with the regulations of the state cyberspace authority regarding standard contracts" rather than directly requiring the use of "standard contracts formulated by the state cyberspace authority" as was signalled by Article 38 of the PIPL. This change could mean more flexibility in cross-border data transfer arrangements, in that the parties could customise their data transfer agreement (**DTA**) so long as the DTA does not deviate from the principles and standards established by the CAC (for example, the requirements in Article 9 of the draft Measures on Security Assessments for the Cross-border Transfer of Data).

Exceptions

Article 35 of the draft Network Data Security Regulations proposes two exceptions to the requirement to meet the General Conditions:

a) where the data processor is required to provide Personal Information abroad for the purpose of entering into and performing a contract to which the data subject is a party; or
b) where the data processor is required provide Personal Information abroad for the purpose of protecting the life, health and property of an individual.

Without question, MNCs would welcome these exceptions, in particular the contract performance exception. However, please note that, in their current form, they only apply to Personal Information and MNCs may consider offering consultation comments to the CAC on the issue of whether the exceptions should be expanded to other types of data, especially considering the broadened application of the cross-border transfer restrictions as mentioned above.

Additional obligations

Based on the current draft, the Network Data Security Regulations would also impose additional obligations on data exporters, including an annual data export security reporting obligation (Article 40). Article 39 (a) also seems to suggest that an internal personal information protection impact assessment report (as required under Articles 55 and 56 of the PIPL) would need to be submitted to the cyberspace authority rather than being an internal document for the company. These additional obligations are generally applicable to all Personal Information exporters with no exception based on the volume or the nature of the exported Personal Information.

Necessity requirement on processing Personal Information by consent

Due to the limitation of other statutory grounds under the PIPL based on which Personal Information may be processed, many MNCs rely on consent as a broad-based ground for processing Personal Information. Where consent is obtained, despite the fact that necessity is a general principle of Personal Information processing the PIPL does not strictly confine the scope of the processing to what is necessary for providing the products or services to the data subject. In fact, Article 16 of the PIPL expressly envisages that the processing of Personal Information is not necessary to the provision of products or services. One could even argue that consent may be seen as an exception to the necessity principle.

However, Article 19 of the Draft Regulations now requires that, even when consent is obtained, the processing must be necessary for the provision of services or for performing statutory obligations. Article 20 of the draft Network Data Security Regulations correspondingly requires that the processing rules published by Personal Information processors specify, among others, that Personal Information is "necessary" for the function of the product or service and describe the impact on the data subject if the processing is refused. These provisions, if they become effective, would likely necessitate significant amendments to the current privacy policies of many market players.

Other points of interest

Other than the above key provisions that may have significant implications for the data management of MNCs, we also note below some other points of interest in the draft:

Article 11 sets out the requirements for an emergency response mechanism in the event of a data incident, including a fairly aggressive timeline for government reporting (for example, within eight hours of a data incident that involves Important Data or Personal Information of more than 100,000 data subjects). It would be important to have a well prepared and rehearsed emergency response policy to avoid a regulatory breach.

Article 13 sets out a list of activities that would trigger a network security review. Interestingly, it differentiates between an overseas listing and a listing in Hong Kong. In the case of an overseas listing, a security review is required if the data processor processes the Personal Information of more than one million data subjects. In the case of a listing in Hong Kong, a security review is only required if national security may be affected.

Article 26 of the Draft Regulations requires a data processor processing the Personal Information of more than one million data subjects to comply with the provisions applicable to Important Data processors under Chapter 4 of the draft Network Data Security Regulations. Such provisions require, among others, the designation of a data protection officer, the establishment of a data security management department, the filing of data briefs with the local CAC, the formulation of data security training plans, and the carrying out of regular data security assessments. This suggests to us that the threshold under Article 52 of the PIPL for designating a Personal Information protection officer may therefore be set at one million data subjects.

Key Contacts in China

Allen & Overy

Victor Ho
Managing Partner of A&O Beijing and Shanghai
Registered Foreign Lawyer, Hong Kong
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

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

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