瀚一律师事务所
HAN YI LAW OFFICES
SUITE 1801, TOWER I, HUAYI PLAZA
2020 WEST ZHONGSHAN ROAD, SHANGHAI 200235, CHINA
TELEPHONE: (86-21) 6083-9800
www.hanyilaw.com

November 17, 2021

Memorandum to: Our Clients

PRC Regulatory Updates: China Released Draft Rules Introducing Stringent Administration of Cyber Data Security

On 14 November 2021, the Cyberspace Administration of China or CAC released the *Cyber Data Security Administration Rules* (*Draft for Comments*) (the "Draft") soliciting public comments. The Draft introduced a raft of keenly required implementation details on cyber data security administration as regulated in the *Cybersecurity Law*, *Data Security Law*, and the *Personal Data Protection Law*.

The Draft is widely applicable to businesses and individuals processing data in China, as well as those located outside of China but are involved in certain data processing activities with certain China elements.[1] While the Draft covers substantial details of the rapidly evolving data security regulation in China, this quick alert will share some of our major observations about the Draft from its implications on overseas IPOs, important corporate activities such as M&As, restructurings, and data processing compliance requirements in daily corporate operations, among others.

1. Impact on Overseas IPOs

(1) IPOs in Hong Kong v. Other Jurisdictions

In the *Cyber Security Review Measures* (*revised draft for comments*) (the "CSR Draft") published in July 2021, CAC proposed that companies dealing with personal information of more than one million users should report for cyber security review if they hope to get listed on an overseas stock exchange, triggering extensive speculation as whether such review process would also apply to listings on the Hong Kong Stock Exchange. The Draft seems to have distinguished going public in Hong Kong as opposed to other overseas jurisdictions. It says that companies dealing with personal information of more than one million users must allow the authorities to review their operations if they hope to get listed on an overseas stock exchange, while similar review will only be triggered for a listing on the Hong Kong Stock Exchange when it "will or may affect national security" (irrespective of how many users' data it handles though). The Draft however does not shed light (neither does our telephone inquiries with CAC obtain further information) on what constitutes "national security", which is yet to be spelt out by CAC. From what has been provided in the Draft, companies processing "important data" and "core data" seem to be relatively more likely to be deemed as having a national security

[1] This would include (i) those who offer goods or services in China, (ii) those who analyze, monitor activities of PRC individuals and organizations, (iii) those who process important onshore data, and (iv) other persons provided under relevant laws and regulations.

impact with a higher potential to trigger a cyber security review.

(2) New Obligation of Annual Data Security Assessment and Reporting

The Draft has provided that, data processors get listed on an overseas stock market (which as it reads may possibly include listing in Hong Kong and other overseas jurisdictions) should conduct an annual data security assessment on their own or by an entrusting data security service provider, and report the previous year's data security assessment to the CAC local counterpart at the municipal level by January 31 of each year. This new requirement applies to all overseas listed companies involving in data processing notwithstanding how many personal users' data they handle or whether the national security is involved.

2. M&As, Restructurings and etc.

According to the Draft, if a data processor involves in such important corporate activities as merges, restructures, separations, the data receiver shall continue to fulfill the relevant data security obligations. Further, if it involves important data and more than one million personal users' information, it shall report to the competent local authorities of such corporate activities. If the data process is an Internet platform operator which handles a large number of data resources concerning national security, economic development or public interest, it shall go through network security review and declaration for such proposed M&A, reorganization or separation, if such action will or may affect national security. Where a data processor is dissolved or declared bankrupt, it shall report the same to the competent authorities and transfer or remove relevant data as may be so required.

3. Highlights of Daily Data Processing Requirements

(1) Personal Data

Compared with the *Personal Information Protection Law* enacted in August 2021, the Draft has provided the following highlights in the protection of personal information area, a key area for the network data security regulation:

- *Substantial openness and transparency*. Data processors are required to formulate explicit rules for the processing of personal data and strictly abide by them. These rules should be displayed in a centralized and public manner, accessible and placed in a prominent position, with clear and specific contents, concise and in plain language, and a systematic and comprehensive description for the processing of personal data to individuals.

- *Specific consent and burden of proof*. The Draft reaffirms the provisions under the *Personal Data Protection Law* that the processing of personal data in certain situations should be subject to the individual's specific consent, which is separately defined as a consent by an individual on a specific personal data processing activity, rather than a general consent on multiple personal data or data processing activities. In addition, the Draft specifically provides that the burden of proof is placed on data processors if the validity of an individual's consent is in dispute.

- *Separate consent is required for personalized recommendations*. The Draft stipulates that Internet platform operators using personal information and algorithms to provide personalized information recommendations to users shall be responsible for the authenticity, accuracy and legality of the information provided, and shall obtain specific consent by the individuals receiving such personal information recommendations, a new requirement not provided in the

Personal Data Protection Law. This requirement will help regulate businesses in the automated marketing.

- *Collection of biometric information*. The Draft provides that data processors should conduct a risk assessment of the necessity and security in biometric personal authentication while applicable, and may not use biological features such as facial geometry, fingerprints, and voice recognition as the sole form of personal identification in order to compel individuals to consent to the collection of their personal biometric information.

- *Protection of personal data*. The Draft reiterates China's priority on the protection of personal data. If a data processor possesses more than one million personal users' data, it should also comply with applicable provisions of the *Cyber Data Security Administration Rules* governing processing of important data.

(2) Important Data

The Draft has followed the *Data Security Law* in adopting a "categorized and graded" data governance system, i.e., one that has categorized the relevant data into general data, important data, core data, subject to different levels of security measures according to the impact and importance of the underlying data on national security, public interest or the rights and interests of individuals and organizations. China focuses on the protection of personal information, important data, and core data:

- *Definitions of important/core data and major requirements*. The Draft provides general descriptions of "important data" and "core data" and also enumerates a long list of examples of "important data".[2] Yet more details of the important data and core data would need to be spelt out by the relevant industries and regions in different categories to be released. The processor of important data should, within 15 working days after identifying its important data, file a record of relevant data security details with competent CAC authority. Further, an important data processor should appoint a data security officer, formulate a training plan, conduct annual data security assessments, and report the relevant data security assessments to the competent CAC authority on an annual basis.

- *Consent on sharing*. If a data processor shares, trades or entrusts to process important data, it should obtain the consent from the competent government agency.

(3) *Cross-Border Data Transfer Restrictions*

- *General Restrictions*. China generally requires the storage of data locally within China, and outbound data transfer is generally limited only to required situations for conduct of businesses subject to satisfaction of certain specified conditions (e.g., a cross-border data security assessment has been conducted, or a contract has been concluded with an overseas data receiver in accordance with a standard contract formulated by CAC). This may affect almost all PRC companies in their provision of any data to overseas institutions even for daily

[2] "Important data" includes unpublicized government data, work secrets, intelligence data and law enforcement judicial data, as well as data on safe production and operation, supply chain data on key system components and equipment in such key industries and fields as telecommunications, energy, transportation, water conservancy, finance, defense science and technology, customs, taxation, among others. "Core data" refers to data related to national security, the lifeblood of the national economy and major public interests, and important livelihood data.

business needs, which seems to be much broader than those provided under previous laws and draft rules, and its application is yet to be clarified.

- *Security assessment*. If an outbound data transfer involves important data, the operators of critical information infrastructure and data processor of more than one million users' personal data, it should be subject to a cross-border data security assessment as organized by CAC.

- *Individual consent on personal data*. If a data processor provides personal data to any entity located outside of China, it should obtain consent from the concerned individual and inform him or her of the details of such personal data so provided (e.g., name and contact information of the receiver, purpose and mode of processing, category and manner of personal information so provided).

- *Annual report*. Data processors who provide personal data and important data abroad should prepare a data outbound security report to the competent CAC agency by January 31 of each year of data outbound activities in the previous year.

- *Illegal VPN service is prohibited*. China establishes a cross-border security gateway for data to block unlawful dissemination of information from outside world. No individual or organization may provide programs, tools, and etc. to penetrate or bypass cross-border security data gateways.

(4) Internet platform operators

More burdens have been put on the Internet platform operators:

- *Reporting obligations for overseas operations*. If a large-scale Internet platform operator (i.e., an Internet platform operator with more than 50 million users, processing large amount of personal data and important data, or with strong social mobilization capabilities and market dominance position) sets up overseas headquarters, operation or R&D center, it should report the same to the competent CAC and other government agencies.

- *Disclosure of algorithmic policies*. Internet platform operators should formulate platform rules, privacy policies and algorithmic policies disclosure rules relating to the data, and timely disclose formulation procedures and adjudication procedures. For the formulation of and major amendments to such rules and policies, Internet platform operators should solicit public opinions before adopting the relevant rules and policies.

- *Compensation for third-party liability*. Internet platform operators should assume responsibility for data security management of third-party products and services provided through their platforms (it should clarify third-party data security responsibilities through contracts, etc.), and urge third parties to strengthen data security management and take necessary data security protection measures. If any third party product or service causes damage to a user, the user may request the Internet platform operator to pay the compensation directly on behalf of such third party in advance.

(5) Critical information infrastructure operators ("CIIOs")

Cloud computing services procured by any CIIO (as well as by government agencies) should be subject to security assessment organized by CAC in conjunction with other relevant departments under the State Council.