Legal Commentary

November 16, 2021

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Impact of Draft Internet Data Regulation on Overseas Listings

Authors: Han Kun Law Offices Kevin DUAN | Tracy ZHOU | Kemeng CAI
Han Kun's Hong Kong Associated Law Firm Charles WU

On 14 November 2021, the Cyberspace Administration of China ("**CAC**") published the network Internet Data Protection Draft Regulations (Draft for Comments) (the "**Draft Regulations**"). The Draft Regulations build on the foundations set by the Personal Information Protection Law, the Data Security Law, and the Cybersecurity Law. The Draft Regulations establish a comprehensive set of regulations to implement the protection of personal information and "important data" protection provisions set out in those laws. The Draft Regulations answer certain questions not addressed by the Measures for Cybersecurity Reviews (Draft for Comment) ("**Draft Measures**"), also issued by CAC in July 2021. This article is the first in a series of Han Kun interpretations of the Draft Regulations, and will focus on the potential impact of the Draft Regulations on the overseas listing of PRC companies.

Cybersecurity review requirements: preferential treatment for Hong Kong listings and the application obligation triggered by 1 million users' personal information

Previously, Article 6 of the Draft Measures stated that "[a]n operator that applies for a listing in a foreign country must apply to CAC for a cybersecurity review if it is in possession of the personal information of more than 1 million users". A common inquiry raised by the Draft Measures is whether "a listing in a foreign country" includes a listing in Hong Kong. As the Draft Measures used the unusual concept of "listing in a foreign country" (typically understood to mean outside of China, thereby excluding Hong Kong, as opposed to "listing overseas", which is typically understood to mean outside of China Mainland, thereby including Hong Kong), the market speculated that regulators may have been looking to give Hong Kong listings preferential treatment.

However, the Draft Regulations confirm that Hong Kong listings may also be subject to cybersecurity reviews. While the obligation to apply for a cybersecurity review based solely on the amount of personal information it possesses is retained for companies listing in a foreign country, a different provision of the Draft Regulations regulates Hong Kong listings. Namely, for Hong Kong listings, the obligation to apply for a cybersecurity review will only arise when the Hong Kong listing has national security implications. Article 13 of the Draft Regulations states that "data handlers carrying out the following activities shall, in

accordance with the relevant national regulations, apply for a cybersecurity review: (1) the merger, reorganization and spin-off of Internet platform operators[1] who possess substantial data resources related to national security, economic development and public interests that affect or may affect national security; (b) data handlers that process the personal information of more than 1 million users listing in a foreign country; (c) **data handlers listing in Hong Kong, which affects or may affect national security**; (d) other data processing activities that affect or may affect national security ....."

Unfortunately, the Draft Regulations did not define the scope of and threshold for determining what "affects or may affect national security". If the Draft Regulations come into effect as currently written, PRC companies may have to apply for cybersecurity reviews prior to a Hong Kong listing out of precaution. This means that the so-called preferential treatment for Hong Kong may be limited in practice.

For data handlers listing in a foreign country, like the US, as long as they "process the personal information of more than 1 million users", they must apply for a cybersecurity review with the Office of Cybersecurity Review. Like the Draft Measures, the Draft Regulations do not explicitly require data handlers that process data other than personal information, like "important data" or "core data", to apply for a cybersecurity review prior to listing in a foreign country. However, if these companies do list in a foreign country, they may nevertheless be subject to cybersecurity reviews under the provision "other data processing activities that affects or may affect national security".

We note that the Draft Measures established an all-encompassing operator pool for pre-listing cybersecurity reviews through the use of the relatively more ambiguous concept of "holding" as opposed to "possessing". That is, operators that were holding 1 million users' personal information were subject to a cybersecurity review. The Draft Regulations limits the operator pool to "data handlers", or individuals and entities that have the ability to decide on the purpose and method of data processing activities[2]. However, whether this means relevant operators that primarily process data under client instructions in the course of their businesses (such as cloud service providers, who would ordinarily not be considered "data handlers" under the Draft Regulations) are exempt from cybersecurity reviews remains uncertain and is subject to further clarification from the regulators.

Additionally, the Draft Regulations do not clarify what "listing" means. In this regard, we maintain our view from our previous analysis of the Draft Measures, namely that apart from IPOs, other routes to listing in the US undertaken by Chinese companies, such as SPACs (Special Purpose Acquisition Companies), RTO (Reverse Takeovers), direct listings etc., may all be subject to cybersecurity reviews. Furthermore, with respect to Chinese companies already listed in the US that intend to complete a secondary listing in Hong Kong, in light of the fact that they may need to disclose or provide additional information in accordance with the Listing Rules of Hong Kong, coupled with the fact that they will be subject to the supervision and investigation by the Stock Exchange of Hong Kong and securities regulatory authorities, we take the view that they will need to apply for a cybersecurity review prior to a secondary listing in Hong Kong if such listing "affects or may affect national security".

[1] Internet platform operators means data processors who provide digital-platform related services for its users, such as information distribution, social networking, transaction, payment and audio-visual services.

[2] Draft Regulations Article 73.

Annual data security review and submission obligations for companies listed overseas

In addition to the cybersecurity review, the Draft Regulations also require Chinese companies already listed overseas (including Hong Kong) to complete an annual data security review and report it to regulators. Article 32 of the Draft Regulations stipulates that **data handlers** processing "important data"[3] or **listed overseas** shall conduct an annual data security review **by itself or by commissioning a data security service provider** and submit the annual data security review report from the prior year to the municipal cybersecurity department by 31 January each year. We understand that the phrase "data handlers listed overseas" includes data handlers currently in the process of listing and those already listed overseas.

For a data handler currently going through the listing process, if the foregoing requirements trigger a cybersecurity review obligation, such data handler must consider its obligation to apply for a cybersecurity review and to conduct annual data security reviews. For data handlers that do not meet the foregoing requirements, they will still need to conduct an annual data security review and submit corresponding reports as required.

As for data handlers that are already listed overseas, based on an interpretation of the Draft Regulations alone, the Draft Regulations may not be applied retroactively to require such data handlers to re-apply for a cybersecurity review. However, regardless of whether they process the personal information of more than 1 million users or whether the processing activities have national security implications, such data handlers already listed overseas will now be required to submit annual data security review reports each year to the municipal cybersecurity department by 31 January.

According to the Draft Regulations, the annual data security review report must contain the following: (1) status of important data processing; (2) data security risks identified and mitigation measures; (3) data security management system, data backup, encryption, access control and other security protection measures, as well as the effectiveness of the implementation of such management system and protection measures; (4) implementation of national data security laws, administrative regulations and standards; (5) occurrence of data security incidents and their handling; (6) **an assessment of the security situation with respect to the sharing, trading, third party processing or provision of important data overseas**[4];

[3] Article 73 of the Draft Regulations states that: **important data** refers data that may endanger national security and public interests if tampered with, destroyed, leaked or illegally obtained or illegally used. The following are included: 1. unpublished government data, work secrets, intelligence data and law enforcement and judicial data; 2. export control data, data related to core technologies, design plans, production processes and other data related to export control items, data on scientific and technological achievements in the fields of cryptography, biology, electronic information and artificial intelligence that have a direct impact on national security and economic competitiveness; 3. data that the State laws, administrative regulations and departmental regulations clearly require to protect or control the dissemination of. 4. data on the safe production and operation of key industries and fields such as industry, telecommunications, energy, transportation, water conservancy, finance, national defense science and technology industry, customs, taxation, etc., and data on key system components and equipment supply chain; 5. data on the scale or precision of the relevant State departments, national basic data on population and health, natural resources and the environment, such as genetics, geography, minerals, meteorology, etc.; 6. Data on the construction and operation of national infrastructure, critical information infrastructure and their security, and data on the geographical location and security of important and sensitive areas such as national defense facilities, military administration areas and defense scientific research and production units; 7. Other data that may affect national political, territorial, military, economic, cultural, social, scientific and technological, ecological, resource, nuclear facilities and 7. other data that may affect the security of the country's political, territorial, military, economic, cultural, social, scientific and technological, ecological, resource, nuclear facilities, biological, space, polar, deep sea, etc.

[4] According to Article 32, if a data processor listed overseas carries out the sharing, trading, third party processing or

(7) complaints related to data security and their follow-up measures; (8) other data security related matters as specified by CAC and competent regulatory departments.

Reporting obligation during the reorganization process for an overseas listing

The Draft Regulations also introduce a new reporting obligation for data handlers whose reorganization involves important data and the personal information of more than 1 million users. In other words, if such data handler needs to restructure for whatever reason during the listing process, it may be required to report the reorganization in accordance with the relevant regulations. Article 14 of the Draft Regulations states that in the event of a merger, reorganization or spin-off of a data handler, the data recipient shall continue to fulfil its data security protection obligations, and the data handler shall report the merger, reorganization or spin-off to the competent authorities at the district municipal level if there is important data and the personal information of more than 1 million users. In the event of a dissolution or declaration of bankruptcy of a data handler, it shall report the dissolution or bankruptcy to the competent authorities at the district municipal level where the data handler is located, and the data shall be handed over or deleted in accordance with the relevant requirements. In the event the competent department is unclear, the data handler shall make a report to the municipal cyberspace administration authority.

Interpretations of what constitutes "important data and the personal information of more than 1 million users" may differ. A narrow reading suggests that only the transfer or "divestiture" of important data and the personal information of more than one million users as a result of a merger, reorganization or spin-off (e.g., the transfer of important data and the personal information of more than 1 million users from one entity to another in the course of a reorganization involving the transfer of a business and assets prior to a listing) is subject to this article[5]. However, a broad reading suggests this article and its reporting obligation applies to the reorganization of a group so long as the group processes important data and the personal information of more than 1 million users, even if such data is not actually transferred between entities within the group or if the data handler entity is not a participant in the relevant reorganization. If this is the case, then common reorganization activities such as the creation and removal of red-chip structures may all be required to be reported to the municipal authorities of CAC.

Conclusion

As the Draft Regulations continue to uphold the low threshold of "the personal information of more than one million users" as previously set forth in the Draft Measures, a prior application for a cybersecurity

provision of important data overseas, the data security review shall focus on assessing the following: (1) whether the sharing, trading, third party processing or provision of data overseas, as well as the purpose, manner and scope of data processing by the data recipient, are legal, legitimate and necessary; (2) the sharing, trading, third party processing or provision of data overseas faces risks of data leakage, destruction, tampering and misuse and the risk to national security, economic development and public interest; (3) the background information on the data recipient, including the recipient's integrity, law-abiding status, cooperative relationship with foreign government agencies, whether it is sanctioned by the Chinese government, the responsibilities it undertakes and its ability to fulfill its responsibilities, etc., and whether it can effectively guarantee data security; (4) whether the data security requirements in the relevant contracts with the data recipient can effectively bind the data recipient to fulfill their data security protection obligations; (5) whether the management and technical measures in the data processing process can prevent risks such as data leakage and destruction. The data processor shall not share, trade, engage in third party processing or provide data overseas if the assessment concludes that the data may endanger national security, economic development and public interests.

[5] Article 14 uses the concept of 'data recipient', which is usually used in the context of data transfer.

review will effectively become a standardized procedure for Chinese companies with personal information that hope to list in the US in the future. For Hong Kong listings, although the Draft Regulations set the seemingly lenient provision of "affecting or may affect national security", the specific requirements in practice have yet to be clarified by regulators. In addition, the annual data security review and reporting requirements for overseas issuers, as well as the reporting requirements of data handlers for mergers, reorganizations and spin-offs as set out in the Draft Regulations, will become compliance obligations for Chinese companies both before and after their overseas listing.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com

Tracy ZHOU

Tel: +86 10 8525 5512
Email: tracy.zhou@hankunlaw.com

Charles WU

Tel: +852 2820 5617
Email: charles.wu@hankunlaw.com