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

Han Kun Newsletter

Issue 175 (11th edition of 2021)

Legal Updates

1. CAC Releases Draft Data Export Security Assessment Rules for Public Comments
2. Impact of Draft Internet Data Regulation on Overseas Listings

1. CAC Releases Draft Data Export Security Assessment Rules for Public Comments

Authors: Kevin DUAN | Kemeng CAI | Yuting WANG

On October 29, 2021, the Cyberspace Administration of China ("**CAC**") released for public comments a draft of the *Measures for Security Assessment of Data Export* ("**Draft**"). The Draft aims to refine and implement Article 37 of the Cybersecurity Law, Article 31 of the Data Security Law, Articles 36, 38, and 40 of the Personal Information Protection Law, and provisions of other laws related to data exports. Compared with previous draft rules and standards[1], the Draft reflects a strict position toward data export administration; for example, the Draft sets a lower data quantity threshold for government assessments, requiring enterprises to adhere to a combination of pre-assessments and continued supervision as well as a combination of risk self-assessments and security assessments, centralizing the authority of security assessments up to the level of the CAC. Correspondingly, the Draft also provides for serious consequences in the case of non-compliance—entities would be required to cease data export activities where they fail to apply for re-assessment when prescribed circumstances occur during the two-year validity period for assessment results or as required by the expiration of the validity period.

The purpose of this article is to briefly analyze from an enterprise data export perspective the notable issues and potential challenges posed by the Draft.

Wide scope of application

Article 2 of the Draft stipulates that data handlers that provide important data collected and generated during operations within China and personal information subject to security assessments according to law are required to conduct security assessments in accordance with the provisions of the Draft. Article 4 further specifies five circumstances that require applying for a government assessment.

- Personal information and important data collected and generated by operators of critical information infrastructure. (corresponding to Article 37 of the Cybersecurity Law);
- The data to be exported contains important data;
- Personal information handlers who process personal information of at least one million individuals provide personal information cross-border;
- Cumulatively transfer cross-border personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals;
- Other situations determined by the CAC authorities that require data export security assessments.

[1] The CAC announced a draft of the *Measures for Security Assessment of Personal Information and Important Data Exports* in 2017, the National Information Security Standardization Technical Committee published a draft of the *Guidelines for Data Cross-border Transfer Security Assessment* in 2017, and two years later the CAC announced a draft of the *Measures for Security Assessment of Personal Information Export* in June 2019.

The most important highlight of the Draft is that it specifies a personal information quantity threshold called for in Article 40 of the Personal Information Protection Law, which requires government assessments for "CIIOs and personal information handlers processing personal information reaching quantities provided by the CAC authorities". In addition, the Draft reiterates security assessment requirements for data exports by critical information infrastructure operators in Article 37 of the Cybersecurity Law and the continued strengthening of regulations for exports of important data.

In practice, a question enterprises often raise is whether the prescribed quantity in Article 40 is based on the quantity of personal information held by the enterprise (or enterprise group), the quantity of personal information processed by the relevant information system, or the quantity of personal information provided in specific processing activities. In this regard, the Draft proposes two standards: "amount processed" and "quantity provided". The "personal information handlers who process personal information of one million individuals" appears to refer to the total number of information subjects associated with a particular data handler (theoretically, a legal entity) (which may add up the personal information in various systems), while "[cumulatively providing cross-border personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals" appears to refer to the quantity of information subjects associated with the specific provision activities of a particular data handler. Both of these quantity thresholds are set at a low level, and enterprises meeting either would be required to apply for a government assessment.

These low-level quantity thresholds are likely to have a profound impact on cross-border data transfer practices. Multinational companies ("**MNCs**") would need to apply for a government security assessment before transferring personal information outside of China where they provide B2C products or services or where they provide products or services that do not hold consumers' personal data but may employ a large number of employees in China or hold a large number of B-side customer contacts. All enterprises engaging in such data export activities should actively conduct self-examinations to determine whether their processing or cumulative provision of personal information reaches the aforementioned quantity thresholds or involves the export of important data. Once the Draft is adopted and implemented, enterprises that engage in these data exports may be required to apply to CAC authorities for a security assessment.

Self-assessment as a guide

Article 5 of the Draft requires that before providing data cross-border, data handlers must conduct an advance self-assessment of data export risks, which focuses on the following items:

- The legality, legitimacy, and necessity of the purpose, scope, and method of data processing of the data export and overseas receivers;
- The quantity, scope, type, and sensitivity of the data to be exported, and the risks that the exported data may bring to national security, public interests, and the legitimate rights and interests of individuals or organizations;
- Whether the data handler's management and technical measures and capabilities in the data transfer link can prevent risks such as data leakage and damage;

- The responsibilities and obligations promised by the overseas receiver, and whether the management and technical measures and capabilities to perform the responsibilities and obligations can guarantee the security of the exported data;
- Risks of data leakage, damage, tampering, abuse, etc. after the data is exported and re-transferred, whether the channels for individuals to maintain personal information rights and interests are unblocked, etc.;
- Whether the data export-related contracts concluded with overseas receivers fully stipulate responsibilities and obligations for data security protection.

Article 6 prescribes that "data export risk self-assessment reports" and "contracts or other legally binding documents drawn up between the data handlers and overseas receivers" (hereinafter collectively referred to as "**Contracts**") as one of the key materials required to apply for data export security assessments. The latter requires that the Contracts fully stipulate data security protection responsibilities and obligations. Article 9 states that the Contracts must include the following terms:

- The purpose, method and scope of data exports, the purpose and method of data processing by overseas receivers, etc.;
- The location and duration of data storage overseas, and the processing measures for the exported data after the storage period expires, the agreed purpose is fulfilled, or the contract is terminated;
- Binding clauses restricting the transfer of the exported data by overseas receivers to other organizations and individuals;
- The security measures that the overseas receiver should take when the actual control rights or business scope of the foreign party undergo a substantial change, or the legal environment of the country or region where it is located makes it difficult to ensure data security;
- Liability for breach of data security protection obligations and binding and enforceable dispute resolution clauses;
- In the event of data leakage and other risks, properly carry out emergency responses and ensure unobstructed channels for individuals to safeguard their personal information rights.

Government assessment as the core

While attaching importance to Contracts and self-assessments to promote enterprises' self-control of data export risks, the Draft still emphasizes the core role of government pre-assessment of data export security management. All data handlers with the circumstances prescribed in Article 4 are required to apply for government data security assessments before exporting, and the data export security assessment is conducted by CAC authorities. The process of applying for the assessment is as follows:

- Data handlers shall apply to the national CAC authorities through the provincial CAC authorities where they are located, and submit the application materials; (Articles 4, 6)

- The national CAC authorities shall, within seven working days from the date of receipt of the application materials, determine whether to accept the evaluation and feedback the acceptance result in the form of a written notification; (Article 7)
- After the national CAC authorities accept the application, they shall organize competent industry departments, relevant departments of the State Council, provincial CAC authorities, and specialized agencies to conduct security assessments; (Article 10)
- The national CAC authorities shall complete the data export security assessment within 45 working days from the date of issuance of the written acceptance notice; the period can be extended appropriately if the situation is complicated or supplementary materials are required, but generally no more than 60 working days. The results of the assessment will be notified to the data handler in writing. (Article 11)

Article 8 prescribes that government assessments should focus on:

- The legality, legitimacy, and necessity of the purpose, scope, and method of the data export;
- The data security protection policies and regulations of the country or region where the overseas receiver is located and the impact of the network security environment on the security of the exported data; whether the data protection level of the overseas receiver meets the laws, administrative regulations, and national standards;
- The quantity, scope, type, and sensitivity of the data to be exported, and the risks of leakage, tampering, loss, destruction, transfer, or illegal acquisition or illegal use during and after the export;
- Whether data security and personal information rights can be fully and effectively protected;
- Whether the contract between the data handler and the overseas receiver fully stipulates the data security protection responsibilities and obligations;
- Compliance with Chinese laws, administrative regulations, and departmental rules.

Compared with the 2019 draft rules[2], the Draft centralizes the authority of assessment up to the level of the CAC and requires that the competent industry departments be consulted in the process of important data export security assessments. The assessment period is 45 working days after the acceptance of materials, and may be extended to 60 working days or even longer. In practice, the enterprise's data processing activities are usually time-sensitive and continuous, so the longer review period may bring greater uncertainty to the cross-border transfer of various types of customer data and employee data related to enterprise operations.

[2] According to the draft *Measures for Security Assessment of Personal Information Export*, Article 7: "Provincial CAC authorities shall, when notifying the conclusions of security assessment for cross-border transfer of personal information to network operators, report the information on security assessment for cross-border transfer of personal information to the national CAC authorities. Where any network operator raises any objection to the conclusions of security assessment for cross border transfer of personal information drawn by a provincial CAC authority, it may file a petition with the national CAC authorities."

Continuous assessment and supervision

The data export security assessment is not a one-time assessment. The Draft aims to establish a continuous assessment and supervision mechanism. Data handlers can normally carry out data export activities during the two-year validity period for data export assessment results. However, if one of the prescribed circumstances occurs during the validity period or if the validity period expires, the data handler must apply for re-assessment.

Specifically, after a data handler has passed a CAC data export security assessment, it is not required to apply for a re-assessment during the two-year period for subsequent or successive transfers of similar data to the same receiver. However, data handlers are required to apply for a re-assessment in the following circumstances (Article 12, 16):

- The purpose, method, scope, and type of data provided overseas, and the use and method of data processing by overseas receivers have changed, or the overseas retention period of personal information and important data has been extended;
- Changes in the legal environment of the country or region where the overseas receiver is located, changes in the actual control of the data handler or the overseas receiver, changes in the contract between the data handler and the overseas receiver, etc. may affect the data-exporting security;
- If the national cyberspace administration finds that the data export activity that has passed the assessment no longer meets the data export security management requirements in the actual processing process.

As for the situation of "no longer meets the data export security management requirements in the actual processing process", the Draft does not give any further explanation other than the first two situations mentioned above. It remains to be seen in practice whether enterprises will have to apply for a re-assessment when there are any changes in the purpose, mode, scope, type, or use of the data exported or processed outside China, or whether changes in the specific scope and magnitude of the quantity do not require security assessment.

Our comments

The Draft proposes unprecedentedly strict restrictions on cross-border transfers of important data and certain quantities of personal information. Combining the data export security assessment for personal information and important data into one regulation reflects China's caution and concern about the national security risks posed by large quantities of personal information exported from China.

The Draft sets a very low quantity threshold for government assessment of personal information exports, and the regulations and guidelines currently under consultation define important data very broadly. If the Draft is officially issued in its current form, enterprises whose business relies on offshore data processing or centralized storage will come to view data localization as an expensive yet inevitable option to avoid lengthy assessment procedures and the uncertainties arising therefrom.

Not only does the Draft call for structural IT adjustments, internal organizational restructuring, and

consequently enormous upfront investment costs to MNCs in China, it is also likely to generate ongoing compliance costs such as classifying data for export, data cross-border transfer agreement management, and continuous supervision of the subsequent use of exported data. The expected influx of assessment applications may also put pressure on and challenge the review capacity of the CAC. Therefore, we call on regulators to reserve a reasonable transition period for enterprise compliance in the process of implementing the new rules, so that enterprises and regulators can implement the required compliance gradually, reduce the business impact on MNCs, and jointly realize the legal and orderly free flow of data across borders.

2. 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[3] 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

[3] 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.

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[4]. 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".

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"[5] or **listed**

[4] Draft Regulations Article 73.

[5] 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

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**[6]; (7) complaints related to data security and their follow-up measures; (8) other data security related matters

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.

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

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[7]. 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 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.

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

Important Announcement

This Newsletter 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:

Beijing	**Wenyu JIN**	**Attorney-at-law**
	Tel:	+86 10 8525 5557
	Email:	wenyu.jin@hankunlaw.com
Shanghai	**Yinshi CAO**	**Attorney-at-law**
	Tel:	+86 21 6080 0980
	Email:	yinshi.cao@hankunlaw.com
Shenzhen	**Jason WANG**	**Attorney-at-law**
	Tel:	+86 755 3680 6518
	Email:	jason.wang@hankunlaw.com
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com