Legal Commentary

November 25, 2021

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

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

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.

[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.

- 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.

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.

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.

[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."

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.

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