Legal Commentary

July 19, 2022

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

BEIJING | SHANGHAI | SHENZHEN | HAIKOU | HONG KONG

CAC Formally Promulgates the Assessment Measures for Data Export

Authors: Kevin DUAN | Kemeng CAI | Tina WANG | Zihuan XU | Jin JIN

On July 7, 2022, the Cyberspace Administration of China (the "**CAC**") formally promulgated the *Measures for Security Assessment of Cross-border Data Transfers* (the "**Assessment Measures**"), which specify and implement the provisions on data export in accordance with Article 37 of the *Cybersecurity Law of the People's Republic of China* (the "**CSL**"), Article 31 of the *Data Security Law of the People's Republic of China* (the "**DSL**"), and Articles 36, 38, and 40 of the *Personal Information Protection Law of the People's Republic of China* (the "**PIPL**"). The Assessment Measures generally continue with strict supervision toward data exports and adopt the institutional framework proposed in the *Measures for Security Assessment of Cross-border Data Transfers (Draft for Comment)* (the "**Draft Assessment Measures**"), issued by the CAC on October 29, 2021, but relaxed provisions are also found in their details. In this newsletter, we briefly analyze the main contents of the Assessment Measures and highlight notable key issues and potential challenges.

Defining the "export of personal information and important data"

According to Article 2 of the Assessment Measures, applicable data export activities are those where data handlers provide cross-border important data and personal information collected and generated in the course of their operations within China mainland. In addition, the export of de-identified personal information also falls into the application scope of the Assessment Measures in accordance with the definition of personal information stipulated in Article 4 of the PIPL.

As for understanding the "export of personal information and important data", we summarize the applicable data export activities under the Assessment Measures into two categories in line with the introduction of CAC's accompanying press briefing[1], which include: (i) cross-border transfer and storage of data collected and generated in China mainland; and (ii) storing data collected and generated in China mainland, but providing overseas institutions, organizations, and individuals with right of access and use to such data.

[1] CAC's accompanying press briefing published on July 7, 2022, for more details please refer to: http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm (last access on July 8, 2022).

In addition, significant concerns have been raised as to whether the Assessment Measures apply to the circumstances stipulated by Article 3.2 of the PIPL i.e., whether overseas entities' direct collection of personal information from domestic personal information subjects is subject to a cross-border data transfer security assessment ("**Security Assessment**"). The Assessment Measures do not clearly address this issue, and it needs to be further clarified in subsequent supervision practice. However, considering the system interpretation, we tend to take the view that, for personal information, "export" in the Assessment Measures only refers to circumstances where domestic personal information handlers export personal information in accordance with Chapter III of the PIPL. In other words, an overseas entity may not be required to perform a security assessment under the Assessment Measures to directly collect personal information from domestic personal information subjects. In view of the uncertainty in the application scope of the Assessment Measures, it is advisable for relevant enterprises to pay close attention to regulatory developments and to consider obtaining a personal information protection certification when collecting personal information directly from domestic personal information subjects, in accordance with the *Practice Guidelines for Cybersecurity Standards - Technical Specifications for the Certification of Personal Information Cross-border Processing,* officially issued by the Secretariat of the National Information Security Standardization Technical Committee on June 24, 2022.

Circumstances subject to the application for Security Assessment

Article 4 of the Assessment Measures specifies four circumstances subject to the Security Assessment, which are:

- data handlers who export important data;
- critical information infrastructure operators or personal information handlers who export personal information and have processed the personal information of at least 1 million individuals;
- data handlers who have cumulatively exported personal information of at least 100,000 individuals or sensitive personal information of at least 10,000 individuals since January 1 of the previous year;
- other circumstances where an application for Security Assessment is required as prescribed by the CAC.

The following are key points for these applicable circumstances.

I. All exports of important data are subject to the Security Assessment[2]

[2] According to Article 19 of the Assessment Measures, important data are those data that once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and safety, etc. The Assessment Measures do not clearly list specific types of important data, so the identification of important data still needs to be clarified in accordance with other laws, regulations and standards. Based on the DSL each region or department is responsible for formulating a specific catalog of important data in its own region, department, and relevant industries and fields. The National Information Security Standardization Technical Committee has begun to formulate relevant national standards since 2020, and the *Information security technology - Guideline for identification of critical data (Draft for Comments)* has been reviewed and revised for several rounds as of January 7, 2021, which will provide principal guidance for the formulation of specific catalogs of important data in each region and department. Among industry regulations, the *Several Provisions on Automotive Data Security Management (Trial Implementation)* applied to the automotive industry define important data (involved in the process of automobile design, production, sales, use, operation and maintenance) as the data that, once tampered with, destroyed, leaked or illegally obtained or illegally used, may endanger national security, public interest or the legitimate rights and interests of individuals and organizations, and

According to Article 31 of the DSL, the CAC is entitled to formulate regulations for the export of important data. Accordingly, Article 4 of the Assessment Measures requires all circumstances where data handlers export important data to be subject to an application for Security Assessment, which indeed broadens the application scope of Security Assessment with respect to important data exports stipulated by Article 37 of the CSL.

II. The thresholds for determining personal information exports is limited to a maximum of two years

Overall, the Assessment Measures follow the cumulative thresholds proposed by the Draft Assessment Measures for determining the quantities of personal information processed or exported. However, the export thresholds for personal information of 100,000 individuals and sensitive personal information of 10,000 individuals are considered on a rolling basis from January 1 of the previous year. In other words, the thresholds are determined over a maximum period of two years and these quantities are not accounted for on a perpetual basis. This will reduce compliance costs for small businesses whose quantities of personal information exported are relatively small.

Relationship between local storage and the Security Assessment

Controversy exists as to whether enterprises are required to localize their personal information in China under Article 40 of the PIPL if they meet one of the thresholds for processing or exporting personal information under the Assessment Measures. We take the view that although the Assessment Measures do not explicitly mention a localization requirement, Article 40 of the PIPL expressly stipulates that "critical information infrastructure operators" or "personal information handlers who process personal information meet the threshold prescribed by the CAC" are required to perform two data export obligations, namely "local storage" of personal information collected and generated in China and passing a "Security Assessment" when it is indeed necessary to export such data. Therefore, theoretically, localization is in essence a mandatory obligation of enterprises that meet the quantity threshold prior to export. In addition, local storage also helps competent authorities to carry out more efficient supervision of data security. However, considering the low quantity threshold set by the Assessment Measures, it remains to be seen in practice whether the competent authorities will strictly require "local storage" to pass the Security Assessment. Because the lengthy process of the Security Assessment and the uncertainty of its results, data localization (i.e., local storage and avoidance of data exports) may become an option forced upon many enterprises.

Self-Assessment as a precursor

As for the cross-border data transfer risk self-assessment requirement (the "**Self-Assessment**"), Article 5 of the Assessment Measures stipulates that "data handlers shall carry out [Self-Assessments] before applying for the [Security Assessment]". The matters to be assessed include the legality, legitimacy and necessity of the export as well as the purpose, scope, and method of the data processing of overseas receivers; the quantity, scope, type, sensitivity and risk of data exported; the protection capabilities of

list the specific types of such important data.

overseas receivers; security risks during and after data cross-border transfer and the protection of personal information rights and interests; and contractual arrangements governing the responsibilities and obligations of both parties for data security and protection in contracts or other legally binding documents drawn up for the data export (collectively, "**Legal Documents**"). As for personal information exports, a similar internal assessment requirement is also stipulated in Article 55 of the PIPL and the *Provisions on the Standard Contract for the Export of Personal Information (Draft for Comment)* (the "**Draft Provisions**"), both of which require data handlers to carry out a personal information protection impact assessment before exporting personal information. In practice, we take the view that enterprises may integrate internal assessment processes. That is, enterprises may first carry out a personal information protection impact assessment, and on such basis complete the Self-Assessment in accordance with the Assessment Measures. In general, regardless of whether the enterprise is a critical infrastructure operator or meets a quantity threshold related to personal information, a prior internal assessment is a necessary compliance requirement that must be fulfilled before exporting personal information and important data.

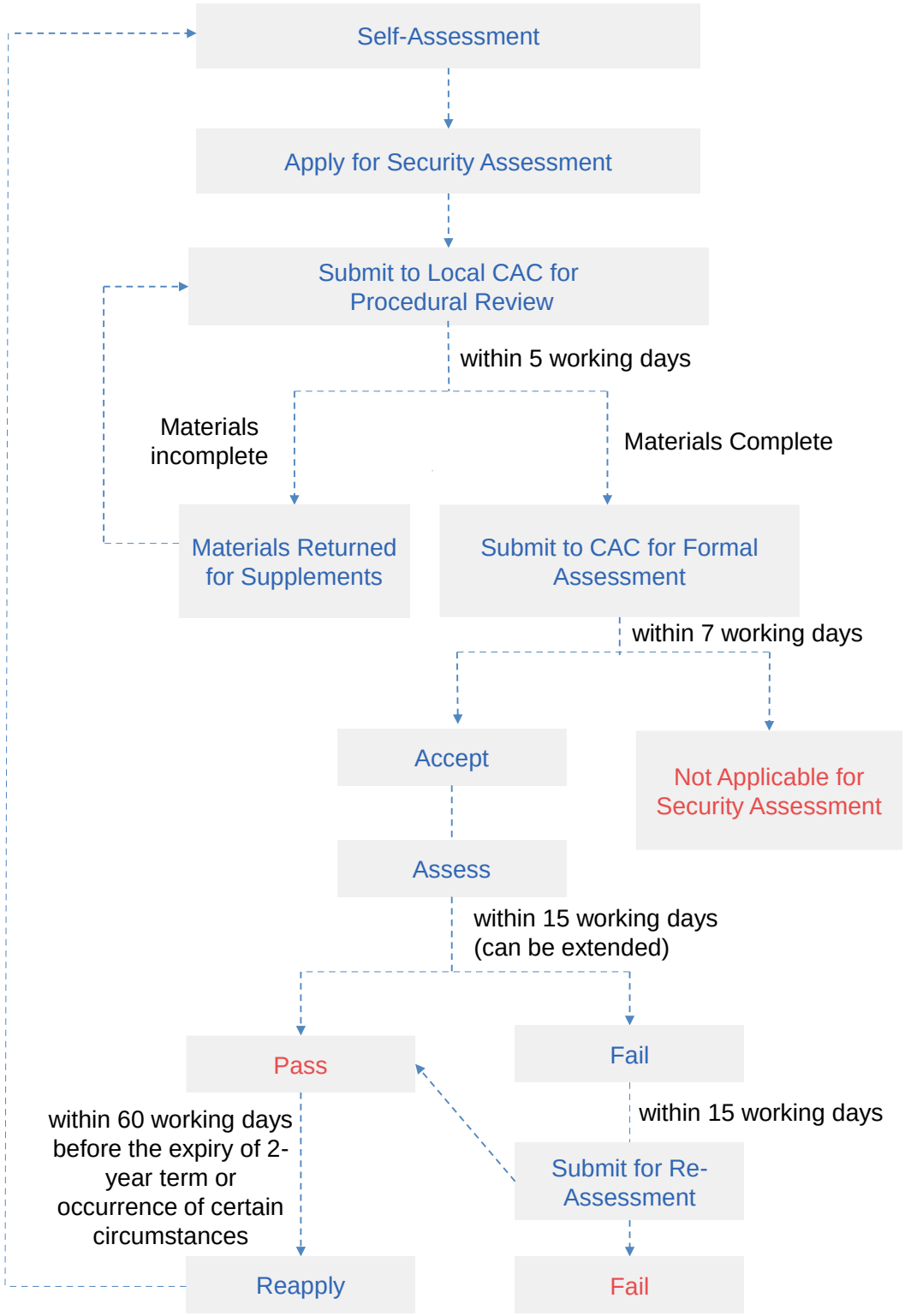
Draw up data export legal documents before applying for the Security Assessment

Data handlers will be required to submit Legal Documents for data export drawn up with overseas receivers when applying for the Security Assessment. According to Article 9 of the Assessment Measures, the Legal Documents include the following terms: the purpose, method and scope of data export; the processing of overseas receivers; the status of data stored overseas; 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 or business scope of overseas receivers undergo a substantial change, the data security protection policies and regulations and the cybersecurity environment of the country and region where it is located; changes or other situations caused by force majeure occur; remedies and liabilities for breaches of data security protection obligations and dispute resolutions; and emergency response requirements and channels for individuals to safeguard their exercise of personal information rights.

The Draft Provisions, together with the *Draft Standard Contract for the Export of Personal Information*, could serve as references for the template contract (for the export of personal information) or important references (for the export of important data). Apart from contracts, other legally binding documents may include unilateral commitment letters from overseas receivers or the data security management systems or policies formulated by corporate groups of domestic data providers and overseas receivers. However, as CAC's accompanying press briefing introduces, data handlers should not formally sign the Legal Documents with their overseas receivers until they pass the Security Assessment; otherwise, they should instead make contractual arrangements that condition the effectiveness of such Legal Documents on passing the Security Assessment.

Rigorous procedures of the Security Assessment

According to Articles 7 and 11-14 of the Assessment Measures, detailed procedures for the Security Assessment are illustrated by the following diagram:



Key points of the aforesaid procedures are as follows:

I. Procedural review by the local CAC

Compared to the Draft Assessment Measures, Article 7 of the Assessment Measures adds a procedure for the CAC at the provincial level to undertake a preliminary review of the completeness of application materials within five working days of the date of receipt. After this procedural review, the provincial-

level CAC will submit the application materials to the CAC, unless it requires the data handler to supplement its application materials if they are found to be incomplete.

II. Removal of the maximum extension period for the Security Assessment

Notably, Article 12 of the Assessment Measures removes the 60-working-day maximum extension period for the Security Assessment stipulated by Article 11 of the Draft Assessment Measures. According to Article 12 of the Assessment Measures, the CAC may extend the assessment for an appropriate period and notify the data handler accordingly, where it finds the case is complicated or there are materials to be further supplemented or corrected. However, there is no explicit limit for this "appropriate period". Therefore, while the assessment period is generally 45 working days, it may be further extended to more than 60 working days. In practice, the data processing activities of enterprises are usually time-sensitive and continuous, so a lengthy assessment period may bring greater uncertainty to the export of various customer data and employee data related to enterprises' operations.

III. Three outcomes of the Security Assessment

There are three possible outcomes of the Security Assessment. First, the Security Assessment is not applicable, in which case the CAC will notify the data handler within seven working days of receiving the application materials that the data export is not subject to the Assessment Measures. In other words, the data handler could then carry out its data export through other lawful means. Second, the data handler passes the Security Assessment, in which case the data handler will be allowed to carry out the data exports upon receiving written notice and strictly in accordance with its application. Third, the data handler fails the Security Assessment, in which case the data handler is prohibited to conduct the data export and must revise its data export plan (such revisions may include reducing the scope or frequency of data export or enhancing the security protection measures after data export) and then reapply for the Security Assessment or adopt data localization measures to avoid exporting the data.

IV. Supplementing procedures for objection and re-assessment

Article 13 of the Assessment Measures adds a procedure for objection and re-assessment on the basis of the Draft Assessment Measures. A data handler who has an objection to the assessment results may apply for a re-assessment to the CAC within 15 working days of the date of receipt of the assessment result; the result of the re-assessment is final. This new procedure provides an additional remedy for enterprises that fail an initial Security Assessment.

Focus of the Security Assessment

Overall, according to the Assessment Measures, the focus of CAC when conducting the Security Assessment is consistent with that stipulated under the Draft Security Measures. The key points are as follows.

- **Understanding the necessity of the data export:** compared with cross-border data transfers, the alternative choice for data localization usually results in a significant increase in operating cost and great inconvenience; for example, it may be hard for international collaborations on certain

tasks and the use of different IT providers may lead to the inability to interconnect, etc. However, whether such considerations could contribute to the necessity of a data export is controversial in practice.

- **Assessing the impacts of security protection policies and regulations and cybersecurity environment of the country or region where the overseas receiver is located on the security of exported data:** conclusions of the following topics need to be further explored and examined in practice—whether the CAC will make adequacy decisions similar to foreign data protection authorities on the data protection level in a specific country or region; whether the CAC will entrust third-party monitoring agencies or academic institutions to make assessment reports; in particular, in the context of intensified global geopolitical and trade conflicts, whether the restrictions on cross-border data transfer to China or other restrictive measures imposed by other countries or regions will affect the results of a Security Assessment.

Continuous assessment and supervision

The Security Assessment is not a one-time assessment. The Assessment Measures aim to establish a continuous assessment and supervision mechanism by which data handlers can normally carry out data export activities during the two-year validity period of the Security Assessment results. However, if one of the prescribed circumstances occurs during the validity period, or if the validity period of the result expires, the data handler is will be required to re-apply for a Security Assessment.

Specifically, after a data handler has passed the Security Assessment conducted by the CAC, it is not required to re-apply during the two-year period for subsequent or successive transmissions of similar data to the same receiver. However, data handlers will be required to re-apply for a Security Assessment in the following circumstances (Articles 14, 17):

- where 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;
- where the data security protection policies and regulations and the cybersecurity environment of the country and region where the overseas receiver is located have changed, or other situations caused by force majeure have occurred, the actual control of the data handler or the overseas receiver has changed, or changes in the Legal Documents between the data handler and the overseas receiver, etc. may affect the security of the data export;
- other circumstances that may affect the security of the data exported;
- where the CAC finds the data export activity that passed a Security Assessment no longer meets the data export security management requirements in actual processing.

Cure period

The Assessment Measures will become effective on September 1, 2022 (the "**Effective Date**"). Compared to the Draft Assessment Measures, Article 20 of the Assessment Measures provides a cure

period for data handlers to rectify within six months any non-compliance in existing data export activities carried out before the Effective Date, i.e., before March 1, 2023. Therefore, data export activities subject to the Assessment Measures but carried out before the Effective Date will not be currently affected. However, relevant data handlers should apply for the Security Assessment as soon as possible to ensure relevant ongoing data export activities are in compliance with laws and regulations.

Our comments

The Assessment Measures propose unprecedentedly strict restrictions on the export of important data and certain quantities of personal information from China mainland. Combining the Security Assessment for personal information and important data into one regulation reflects China's caution and concern over the national security risks posed by exporting large amounts of such data. In summary, the Assessment Measures will not only bring structural IT adjustments, internal organizational restructuring, and the consequent huge upfront investment costs to MNCs in China, but will also generate a lot of continuous daily compliance expenses for processes such as examining data exports, data cross-border transmission agreement management, and continuous supervision of the subsequent outbound use of exported data. To address the compliance challenges posed by the Assessment Measures, it is advisable for enterprises to consider the following suggestions.

- **Consider Local Data Storage**: the Assessment Measures set low quantity thresholds for the mandatory Security Assessment; as a result, enterprises whose businesses presently rely on overseas data processing or centralized storage will inevitably need to consider localization as an option to avoid lengthy assessment procedures and the uncertainty that they bring.
- **Improve internal systems and prepare relevant templates**: the Assessment Measures do not set a maximum time limit for the assessment period, which will bring uncertainty and high potential time costs to enterprises' data export activities. Enterprises who intend to carry out data export activities in the future are advised to formulate an internal data export identification system and a self-assessment system and to prepare relevant Legal Documents in advance, which will serve as key components to smoothly promote data export activities.
- **Carry out data mapping, apply for a Security Assessment as early as possible, and complete rectifications within the cure period**: the cure period is six months after the Effective Date. Before the expiration of the cure period, all enterprises subject to the Security Assessment requirement should begin examining their related data export activities as early as possible and prepare to apply for a Security Assessment in order to avoid the circumstance where the data export activities cannot be carried out upon expiration of the cure period.

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

Kemeng CAI

Tel: +86 10 8516 4289
Email: kemeng.cai@hankunlaw.com