Legal Commentary

September 13, 2022

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

BEIJING | SHANGHAI | SHENZHEN | HAIKOU | WUHAN | HONG KONG

CAC Issues Guidelines for Data Export Security Assessment

Authors: Kevin DUAN | Kemeng CAI | Zihuan XU | Ziqian ZHANG

On August 31, 2022, the Cyberspace Administration of China (the "**CAC**") issued the *Application Guidelines for Security Assessment of Cross-border Data Transfer (1st Edition)* (the **"Application Guidelines"**), which specify and implement the provisions on cross-border data transfer security assessments ("**security assessments**") in the *Measures for Security Assessment of Cross-border Data Transfers* (the "**Assessment Measures**"). The Application Guidelines clarify the application scope of security assessments, stipulate the means, procedures and required materials for the application, and provides contact information for inquiries regarding the application. The Application Guidelines also contain template documents, including the Cross-border Data Transfer Security Assessment Application Letter (the "**Application Letter**") and the Cross-border Data Transfer Risk Self-Assessment Report Template (the "**Self-Assessment Report Template**"), which offer effective guidance and assistance to data handlers who seek a security assessment.

This article briefly analyzes the new requirements set out in the Application Guidelines and highlights critical issues throughout the security assessment application while building on the key points of the Assessment Measures explained in our July 19 article, *CAC Formally Promulgates the Assessment Measures for Data Export.*

Reaffirming the scope of security assessments

The Application Guidelines reaffirm the circumstances subject to mandatory security assessments in accordance with Article 4 of the Assessment Measures[1], and further clarify the criteria for determining cross-border data transfer activities, which is:

[1] Article 4 of the Assessment Measures: "Where a data handler transfers data abroad under any of the following circumstances, it shall, through the local Cyberspace Administration at the provincial level, apply to the State Cyberspace Administration for security assessment for the outbound data transfer: (1) a data handler who transfers Important Data abroad; (2) a critical information infrastructure operator, or a data handler processing the personal information of more than 1 million individuals, who, in either case, transfers personal information abroad; (3) a data handler who has, since January 1 of the previous year cumulatively transferred abroad the personal information of more than 100,000 individuals, or the sensitive personal information of more than 10,000 individuals, or (4) other circumstances where the security assessment for the outbound data transfer is required by the State Cyberspace Administration."

- Data handlers who transfer and store data collected and generated in the course of operations in Chinese Mainland to overseas;
- Data handlers who store data collected and generated in Chinese Mainland, but provide overseas institutions, organizations, and individuals with right of access, retrieve, download and export;
- Other cross-border data transfer activities prescribed by the CAC.

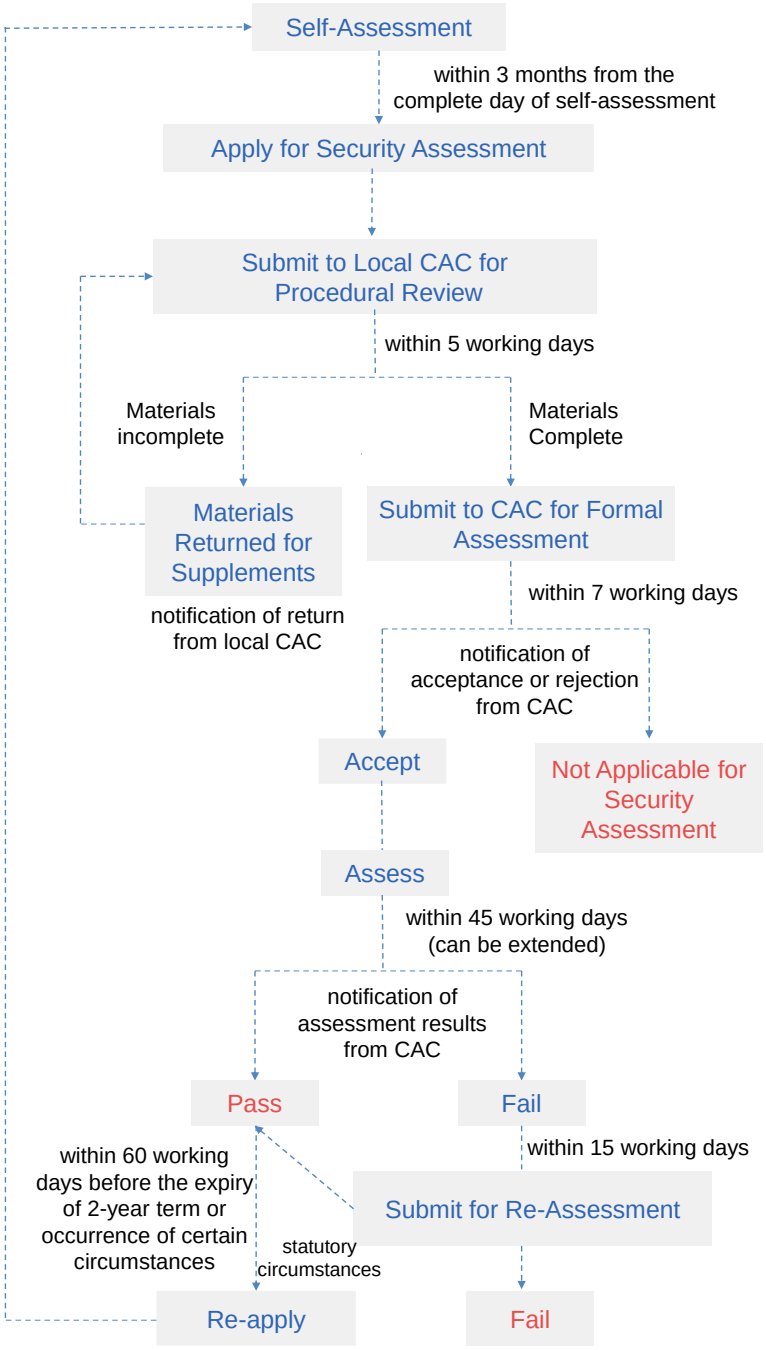
Compared to the CAC's introduction in a press briefing on July 7, 2022[2], in which the second circumstance was described as "provide overseas institutions, organizations, and individuals with the right to access and use such data", the Application Guidelines further specify remote access as "providing overseas institutions, organizations, and individuals with the right of access, retrieve, download, and export".

Notably, the Application Guidelines add a miscellaneous provision to cover "other cross-border data transfer activities prescribed by the CAC", which leaves room for future interpretations when the regulatory authorities deal with complicated data export situations. However, the Application Guidelines do not directly address the direct collection of data from overseas, i.e., where overseas entities directly collect personal information from personal information subjects residing in Chinese Mainland. Therefore, it is advisable for relevant enterprises to closely monitor regulatory developments in this regard and to take corresponding compliance measures when appropriate.

Specifying the application method and procedures

On the basis of Article 7 and Articles 11-13 of the Assessment Measures, the Application Guidelines detail the method and procedures for applying for security assessments with the CAC. The basic process is illustrated by the following diagram:

[2] CAC's press briefing on the Assessment Measures, published on July 7, 2022; for more details, please refer to: http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm (last accessed on September 7, 2022).



Key points of the aforementioned procedures are as follows:

I. Self-assessments must be completed within three months of the date of application

According to the templates provided as annexes to the Application Guidelines, the Letter of Commitment and the Self-Assessment Report Template both require that a cross-border data transfer risk self-assessment ("**self-assessment**") be completed within three months of the date of application, and no significant changes have occurred on or before the date of application.

II. Applications to be submitted on-site

According to Application Guidelines, data handlers will submit application materials to the provincial-level CAC in written form and also attach a digital version. A digital version of materials is to be

submitted via a compact disc.

III. Three types of notifications may be sent during the application process

On the basis of the Assessment Measures, the Application Guidelines provide three notifications that data handlers may receive at three important stages during the application process. These notifications are as follows:

- When data handlers fail to pass the completeness check, the CAC at the provincial level will send a notification to return the materials and to request supplements.
- When the formal assessment is completed, the CAC will send a written notification to inform the data handlers whether their application is accepted.
- When the security assessment is completed, the CAC will send data handlers notification of the assessment results. If there is no objection to the results, the data handlers will regulate their cross-border data transfer activities in accordance with the relevant laws and regulations and requirements stipulated in the notification. In case of any objection, data handlers have a 15-day period to submit for a re-assessment, starting from the date of receipt of the notification of the assessment results, according to Article 13 of the Assessment Measures.

Regarding the official assessment period, Article 12 of the Assessment Measures provides a 45-working-day period, while permitting an extension in the case of complicated situations or material supplements and corrections. However, an abundance of applications may be expected in the short term, given the generally low thresholds for mandatory security assessments as stipulated in the Assessment Measures and the short six-month cure period. Hence, it is possible that the regulatory authorities will not conduct a substantive review in certain cases and permit data exports within a relatively short time for applications that are from less sensitive industries, present a high level of need to engage in cross-border transfer activities, and contain less sensitive outbound data.

IV. Application inquiries may be made

To provide the enterprises a channel to seek official instructions in case of practical problems, the Application Guidelines contain contact information for inquiries related to the security assessment as follows:

- E-mail address: sjcj@cac.gov.cn
- Tel: 010-55627135

As of the date of this newsletter, the Beijing Cyber Administration has set up a hotline for inquiries regarding the security assessment application (010-67676912) and some other provincial-level CACs release their own contact information accordingly. It is advisable for enterprises to take notice of the relevant information disclosed by the regulatory authorities.

Specifying the requirements of the application materials

Compared with Article 6 of the Assessment Measures, the Application Guidelines further specify the

application materials that data handlers should submit when applying for a security assessment and provide corresponding templates, including:

- Photocopy of unified social credit code certificate;
- Photocopy of ID card of the legal representative;
- Photocopy of ID card of the case handler;
- Power of attorney for the case handler;
- Application letter for Security Assessment, including the letter of commitment and the Application Form;
- Photocopies of cross-border transfer related contracts or other legally binding documents to be concluded with the overseas receivers;
- Self-Assessment report on cross-border data transfer risks;
- Other relevant supporting materials.

Key points of the aforementioned materials are as follows:

I. Security assessment "case handler" is introduced for the first time

The Application Guidelines introduces the role of "case handler" for the first time. According to the power attorney for the case handler and the Application Letter of the Security Assessment in the appendix, the case handler shall be the authorized employee of the data handler and in charge of the application work on behalf of the data handler, including filing in the Application Letter of the Security Assessment.

II. Both the data transferor and the data receiver should appoint personnel and a management department responsible for data security

Pursuant to the Application Letter annexed to the Application Guidelines, data handlers need to provide information regarding their personnel and management department responsible for data security and those of their overseas receivers.

This data security personnel and management department requirement is imposed on data handlers who process important data or personal information, and who are critical information infrastructure operators, by Article 27 of *Data Security Law*, Article 52 of *Personal Information Protection Law,* and Article 14 of *Regulation on Protecting the Security of Critical Information Infrastructure*. In addition, *Information security technology-Personal Information Security Specification (GB/T35273-2020)* [3]

[3] Article 27 of Data Security Law: "The carrying out of data handling activities shall be in accordance with laws and regulations, establishing and completing data security management systems for the entire process, organizing and carrying out education and training on data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The carrying out of data handling activities through information networks, i.e., the Internet, shall fulfill the duties to protect data security on the basis of the multi-level protection system for cybersecurity.

Those processing important data shall clearly designate persons responsible for data security and data security

further specifies the criteria for determining whether a person and a department responsible for personal information protection are needed. Building on these laws and regulations, the Application Guidelines require data handlers to fill in the information of data security personnel and management department. However, this may raise the question what information data handlers should provide if they are not required to designate data security personnel and management department under the aforesaid laws, regulations and standard, and we consider such handlers may provide the information of the IT responsible personnel instead.

In addition, it should be highlighted that information should be submitted regarding the personnel and management department of the overseas data receiver. Therefore, enterprises who may be involved in applying for security assessments due to use of overseas data processing services are advised to take into account the conditions of responsible personnel and organization when selecting their service providers. Enterprises should also consider including relevant clauses to guarantee that providers appoint the personnel and department as required, so as to fulfil the requirements of the security assessment.

III. Applications can be made for exports of important data and personal information at the same time

In column "09 Information of Proposed Cross-border Data" in the annexed Application Form, applicants are allowed to fill in the cross-border transfer information of both important data and personal information at the same time. Also, the "Information of Proposed Cross-border Data" section in the Application Letter no longer requires their distinction. This implies that personal information and important data transferred to the same overseas receiver can be the subject of the same application for security assessment. However, it remains unclear whether this is applicable in cases where data is provided to multiple overseas receivers within the corporate group under the same export circumstances, which is an issue facing many multinationals. The Application Guidelines have left this issue for future clarification as the regulations are implemented in practice.

---

management bodies to implement responsibilities for data security protection."

Article 52 of the PIPL: "A personal information processor that processes the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall appoint a person in charge of personal information protection to be responsible for overseeing personal information processing activities as well as the protection measures taken, among others.

The personal information processor shall disclose the contact information of the person in charge of personal information protection, and submit the name and contact information of the person in charge of personal information protection to the authority performing personal information protection functions."

Article 14 of the Regulation on Protecting the Security of Critical Information Infrastructure: "The operator shall set up a special security management organization, and conduct security background examination on the person in charge of the special security management organization and the personnel in key positions. During the review, the public security organ and the state security organ shall provide assistance."

Information security technology personal information security specification (GB/T 35273-2020) 11.1: "Organizations meeting one of the following conditions shall set up full-time personal information protection director and personal information protection work organization to be responsible for personal information security: (1) the main business involves personal information processing, and the number of employees is more than 200; (2) the organization meets one of the following conditions: Processing personal information of more than 1 million people, or expected to process personal information of more than 1 million people within 12 months;(3) Processing sensitive personal information of more than 100,000 people. "

IV. "Legal Documents" defined

Article 8 of the Assessment Measures[4] lists "the legal documents to be concluded between the data handler and the overseas receiver" as one of the key contents of the security assessment, but does not define the "legal documents" concept. The Application Guidelines clearly interpret the concept as "cross-border data transfer-related contracts or other legally binding documents".

Pursuant to the Application Guidelines, to complete the application form, data handlers need to provide the clauses in accordance with the necessary contents one by one as required by Article 9 of Assessment Measures[5].

In view of the strict legal document requirements for a security assessment, it is advisable that enterprises refer to or use the standard contractual clauses of cross-border transfer of personal information issued by the CAC, or ensure that relevant provisions are introduced strictly as prescribed in the Assessment Measures in other legal documents (such as the unilateral letters of commitment from the overseas receiver, or the data security management system or policy of the groups of the parties in Chinese Mainlandor overseas).

In addition, the Application Guidelines clearly state that the Chinese version of legal documents shall prevail. In the case where only a non-Chinese version is available, an accurate Chinese translation is required to be submitted alongside.

V. Compliance with Chinese laws and regulations is highlighted

The Application Guidelines require data handler to submit in its application form its "compliance with Chinese laws, administrative regulations and department regulations". In particular, the data handler is required to briefly describe the administrative penalties and the investigation and rectification by the relevant competent regulatory authorities in its business operations over the past two years, focusing on data security and cybersecurity.

---

[4] Article 8 of the Assessment Measures: "Prior to applying for the security assessment for the outbound data transfer, a data handler shall, in advance, conduct a self-assessment on the risks of the outbound data transfer, and the self-assessment shall focus on the following matters:…(5) whether the responsibilities and obligations for data security protection are fully agreed in relevant contracts for the outbound data transfer, or other legally binding documents to be concluded with the foreign receiver…"

[5] Article 9 of Assessment Measures: "A data handler shall expressly agree on the responsibilities and obligations for data security protection in the Legal Documents concluded with the foreign receiver, which shall, at least, include the following matters: (1) the purpose, method and scope of the data to be transferred abroad, and the purpose and method for processing the data by the foreign receiver; (2) the location and duration for the storage of the data located abroad, as well as how to process the data located abroad upon the expiry of the storage period, achievement of the agreed purpose, or termination of the Legal Documents; (3) restrictions on the foreign receiver's re-transfer of the data located abroad to another organization or individual; (4) security measures which should be taken in case of a material change to the actual control or business scope of the foreign receiver, or in case of a change to the data security protection policies or regulations, or network security environment of the country or region where the foreign receiver is located, or in case that the data security cannot be guaranteed as a result of any other force majeure event; (5) remedial measures, liability for breach of contract and dispute resolution mechanism in the event of a violation of data security protection obligations as agreed in the Legal Documents; and (6) requirements on properly responding to a data security incident, as well as channels and method to safeguard individuals' personal information rights, when the data located abroad is tampered with, destroyed, leaked, lost, transferred, illegally obtained or illegally used."

Providing the Self-Assessment Report Template

According to Article 5 of the Assessment Measures[6], data handlers must conduct a cross-border data transfer risk self-assessment ("**self-assessment**") prior to submitting an application for security assessment. Furthermore, Article 6 requires the data handlers to submit the cross-border data transfer risk self-assessment report to the competent authorities, which means that the self-assessment report is a significant subject of the security assessment process. Annex 4 to the Application Guidelines contains the Self-Assessment Report Template, in which the factual materials to be submitted and evaluation criteria are to be addressed are clarified through instructions.

I. Submission of the Self-Assessment Report

When applying for a security assessment to the CAC at the provincial level, the data handler shall submit a complete and authentic Self-Assessment Report alongside. It should be noted that if a third-party organization involves in the Self-Assessment, its basic information and involvement shall be stated in the Self-Assessment Report. Meanwhile, official seals of the third-party organization on relevant pages are mandatory. Analyzing from the overall requirements of the Application Guidelines, "basic information of the third party organization" may include the name, nature of entity, main business situation, registered address and business address, while "participation" may refer to the work and role of the third party in the Self-Assessment.

II. Coverage and new requirements in the Self-Assessment Report Template

The Self-Assessment Report Template is divided into four parts: a brief introduction of self-assessment work, the overview of cross-border data transfer activities, the risk assessment of proposed cross-border data transfer activities, and a conclusion of the risk assessment.

The first part of the Self-Assessment Report Template mainly summarizes the self-assessment work, including the start and end time, organization, implementation process, and methods, etc. We believe third-party involvement may be disclosed in this section. The second part is intended to cover the business of the data handler and the facts of the cross-border data transfers, including the basic information of the data handler, the design of the transfer business, the conditions of the information systems, the overview of proposed cross-border data transfer, the security assurance capabilities of the data handler, the information of the overseas data receiver, data security protection obligations and responsibilities agreed in the legal documents, and other circumstances the data handler considers

[6] Article 5 of the Assessment Measures: "Prior to applying for the security assessment for the outbound data transfer, a data handler shall, in advance, conduct a self-assessment on the risks of the outbound data transfer, and the self-assessment shall focus on the following matters: (1) the legality, legitimacy and necessity of the purpose, scope and methods of the outbound data transfer, and the processing of the data by the foreign receiver; (2) the scale, scope, type and sensitivity of the outbound data transfer, and the risks to national security, the public interest or to the legitimate rights and interests of individuals or organizations, caused by the outbound data transfer; (3) the duties and obligations which the foreign receiver commits to perform, and whether the foreign receiver's organizational and technical measures and capabilities in terms of performing the duties and obligations can guarantee the security of the outbound data transfer; (4) the risks of the data being tampered with, destroyed, divulged, lost, transferred, illegally obtained or illegally used during and after the outbound data transfer, and whether there is a smooth channel for safeguarding personal information rights and interests; (5) whether the responsibilities and obligations for data security protection are fully agreed in relevant contracts for the outbound data transfer, or other legally binding documents to be concluded with the foreign receiver; and (6) other matters that may affect the security of the outbound data transfer."

necessary to describe. Among them, the "data security protection obligations and responsibilities agreed in the legal documents" are in line with Article 9 of the Assessment Measures concerning the data security protection responsibilities and obligations. It should be stressed that the second part of the self-assessment report has extended the coverage of the material facts related to cross-border data transfers. The added items are as follows:

- In addition to the facts involved in the cross-border data transfer activities, other basic information of the data handler, other than the enterprise information open to the public, are to be submitted, including basic information of organization or individual, information of equity structure and actual controller, information of organization structure, information of data security management department, overall information of business and data, information of domestic and overseas investment;
- The basic information of the facilities that may be involved in the cross-border data transfer activities shall be introduced comprehensively, including information of data assets related to the business of cross-border data transfers, information of information system in Chinese Mainland and overseas, information of data centers (including cloud services) related to cross-border data transfers, information of cross-border data transfer links (such as the provider, number and bandwidth of the links);
- It is necessary to disclose information about providing cross-border data to other overseas receivers through onward transfers after the cross-border data transfer;
- In terms of the security assurance capabilities of the data handler, the self-assessment report builds on the *Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)* and further requires the data handler to illustrate its internal categorization and classification of data, the development of its risk assessment system, as well as its compliance with laws and regulations pertaining to data and cyber security;
- As regards to the overseas receiver, the self-assessment report adds that it shall include a "description of the whole process of data processing by the overseas receiver", which covers the data life cycle from the collection by the overseas receiver from Chinese Mainland, to the use, retention, disclosure and deletion.

The third part of the Self-Assessment Report Template basically restates the requirements of the cross-border data transfer risk assessment in Article 5 of the Assessment Measures, which instructs data handlers to conduct risk assessment based on the facts specified in the second part. Meanwhile, the Self-Assessment Report Template adds a requirement to explain the risk assessment and focus on the problems and potential risks found in the assessment, as well as the corresponding rectification measures and rectification effects. Thus, in addition to the risk assessment of the proposed cross-border data transfer, the data processor also needs to disclose the rectification measures taken to mitigate the risk and the outcomes therefrom.

Our comments

As the Assessment Measures take effect, enterprise cross-border data transfers are entering a phase of compliance rectification, for which the Application Guidelines offer detailed instructions and a roadmap. Pursuant to the Assessment Measures and the Application Guidelines, it is advisable for enterprises to mitigate compliance risks for their data exports by addressing the following:

- Specify the circumstances of cross-border data transfers throughout data processing activities and examine the relevant facts. Determine whether these circumstances fall within the scope of the security assessment and select a data export strategy accordingly (such as to pursue complete data localization or apply for a security assessment as prescribed by laws and regulations);
- Refer to the second part of the Self-Assessment Report Template to conduct a self-assessment in a timely manner. Identify the potential risks and take corresponding mitigation measures so as to pass the security assessment within the six-month period provided in the Assessment Measures;
- Prepare the application materials as required by the Application Guidelines and submit to the relevant CAC at the provincial level, including the photocopy of unified social credit code certificate, photocopy of ID card of the legal representative, photocopy of ID card of the case handler, power of attorney for the case handler, the Application Letter for Security Assessment, including the letter of commitment and the Application Form, photocopies of cross-border transfer related contracts or other legally binding documents to be concluded with the overseas receivers, a self-assessment report, etc.;
- Establish an internal compliance system for cross-border data transfer security assessments. Continue to monitor the conditions of all data exports. Update the submitted materials and re-apply for a security assessment when required.

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