THE CAC ASSESSMENT COLLECTION – PART 3: STEPS AND TIMELINE OF A CAC ASSESSMENT

Date: 20 December 2022

China Data Protection, Privacy, and Security Alert

By: Amigo L. Xie, Dan Wu

In our previous posts, we discussed what data export activities are subject to scrutiny assessment (CAC Assessment) conducted by the Cyberspace Administration of China (CAC) (see Part 1) and examined what companies must do before submitting a CAC Assessment application (see Part 2). In the last article of our CAC Assessment series, we will address the procedures and timeline of a CAC Assessment, the circumstances that trigger a renewal or reapplication of a CAC Assessment, and the consequences of noncompliance.

WHAT ARE THE PROCEDURES AND TIMELINE OF A CAC ASSESSMENT?

The CAC Assessment could take a considerable amount of time. The table below provides a sample timeline for the assessment process based on what is provided for in the *Measures for Security Assessment of Data Exports* (Measures) and the Guidelines on Application of Security Assessment of Data Exports (First Version) (Guidelines):

Step 1A	To conduct a self-assessment	Within **3 months** before the application date
Step 1B	To agree on a draft data transfer contract or other type of legal document (collectively Legal Document) between the data controller and the overseas data recipient	-
Step 1C	To collect and prepare other application documents, including without limitation, an application form[1] and a power of attorney appointing an agent handling the application related matters.[2]	-
Step 2	The provincial office of the CAC to check the completeness of the application materials[3]	**5 business days**
Step 3	The CAC to conduct a preliminary review of the application materials and determine whether to accept the application	**7 business days**
Step 4	The CAC to conduct a formal assessment by involving relevant national and local authorities	**45 business days**, extendable for complicated cases or when additional documents are needed

©2005-2026 K&L Gates LLP. All Rights Reserved.

		from the applicant
Step 5	The CAC to notify applicant in writing, the result of the security assessment	-
Step for Appeal	Applicants, who disagree with the result, may appeal the case to the CAC	Within **15 business days** after CAC's notification

As noted above, it will take time for a data controller to conduct a self-assessment, negotiate a Legal Document with an overseas recipient, and complete a CAC Assessment application form before it can submit an application for a CAC Assessment. It is also possible that the CAC will ask for additional information and documents during the formal assessment process, which could extend the review period from the standard period of a maximum of 57 business days to a longer term. Considering all these factors, the entire CAC Assessment could take longer than three months to complete.

If a data controller has any objection to the assessment result, the data controller may apply for a reassessment within 15 business days of the date of receipt of the assessment result to the CAC, and the result of the reassessment is final.

RENEWAL OF ASSESSMENT UPON THE EXPIRATION OF THE TWO-YEAR TERM

The CAC Assessments, once cleared, will be valid for two years. If a data controller intends to continue to export data, a renewal application must be submitted 60 business days prior to the expiration of the two-year term of validity.

CIRCUMSTANCES THAT COULD TRIGGER RE-APPLICATION BEFORE CLEARANCE EXPIRATION

There are certain circumstances under which a data controller may be required to undergo additional CAC Assessments before the initial clearance expires. For instance, if a company attempts to acquire a target company that engages in data export activities that must be cleared by a CAC Assessment, the target company may need to obtain additional CAC clearance if there is a change in control. This point is particularly important to consider moving forward in change in control transactions in China, and obtaining clearance via an additional CAC Assessment should be an important closing condition in these types of transactions.

Additionally, a data controller could be required to re-apply for a security assessment if there is:

- Any change in the purpose, processing method, scope, or type of the data which affects the security of the exported data, or any change in the retention period of personal data or important data;
- A change in the regulations or cyber security conditions of the home country or region of the data recipient, and a change in the Legal Document between the data controller and the data recipient, in each case affects the security of the transferred data; or
- Other circumstances affecting the security of the exported data.

©2005-2026 K&L Gates LLP. All Rights Reserved.

SUSPENSION OF DATA TRANSFER DUE TO NONCOMPLIANCE

A data controller is required to comply with data transfer regulations on an on-going basis; otherwise, the CAC could order the data controller to suspend all data transfers.

More specifically, after obtaining a clearance from the CAC, the data controller should comply with data export security management requirements on an on-going basis. If the CAC determines that a data controller fails to meet the data export security management requirements after the clearance, the CAC has the power to order the data controller to suspend the data transfer.

TAKEAWAYS

Act Now

The Measures have taken effect from 1 September 2022. For data exported before 1 September 2022, data controllers are given a six months grace period to rectify any noncompliant activities pertaining to data exporting. Given time is necessary to complete a standard CAC Assessment, data controllers that are subject to the CAC Assessment must act now to prepare and submit the application before 1 March 2023.

Localization or Anonymization as Alternatives

For a data export activity that requires a CAC Assessment, companies should consider the time and resources required for it to go through the CAC Assessment and the likelihood for it to obtain clearance from the CAC. Companies may also consider whether it is possible to localize the data or anonymize the personal information involved before a data export activity as options just in case the CAC Assessment is not available.

If you have any questions regarding the issues discussed in this alert including data privacy-related issues, our Global Data Protection team, which includes lawyers across our Greater China region offices, is available to assist with legal and compliance advice, including risk assessments and reviews.

FOOTNOTES

[1] The form requires not only a significant amount of but also sensitive information about an overseas data recipient (e.g., share capital amount, number of employees), which, in practice, many overseas data recipients who are vendors of a data controller might not be willing to provide.

[2] The authorized agent is not allowed to sub-authorize another person to handle the application matter according to a template of the power of attorney provided in the Guidelines.

[3] Several provincial offices of the CAC, such as Shanghai, Jiangsu, Zhejiang, Tianjin, and Hebei, promulgated local guidelines or opened hotlines for the application for a CAC assessment.

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



AMIGO L. XIE
PARTNER OF K&L GATES LLP AND REGISTERED FOREIGN LAWYER

HONG KONG
+852.2230.3510
AMIGO.XIE@KLGATES.COM



DAN WU
COUNSEL

SHANGHAI
+86.21.2211.2083
DAN.WU@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.