THE CAC ASSESSMENT COLLECTION – PART 2: WHAT MUST BE DONE BEFORE APPLYING FOR A CAC ASSESSMENT?

Date: 9 December 2022

China Data Protection, Privacy, and Security Alert

By: Amigo L. Xie, Dan Wu, Prudence Pang, Grace Ye

In a recent alert, we painted the big picture of the security assessment conducted by the Cyberspace Administration of China (CAC) to data exporting activities from China (CAC Assessment), highlighting what data export activities are subject to scrutiny under a CAC Assessment. In this second part of the CAC Assessment series, we will take a deeper look at what companies must do before submitting a CAC Assessment application.

In terms of conditions for companies to fulfil before applying for a CAC Assessment, according to the list of application documents under the *Measures for Security Assessment of Data Exports* (Measures), companies must conduct a self-assessment, present a draft agreement or other type of legal document with a data recipient located overseas, and fulfil other conditions before applying for a CAC Assessment.

A. SELF-ASSESSMENT

To complete the CAC Assessment application, applicants must submit a self-assessment report. Under the *Guidelines on Application of Security Assessment of Data Exports (First Version)* (Guidelines), data controllers must conduct a self-assessment on data export risks within three months before applying for a CAC Assessment.

There is substantial overlap between the factors companies must assess to compile a self-assessment report and what the CAC will consider when conducting a CAC Assessment. In general, the CAC Assessment will consider everything that is required under a self-assessment and three additional items, including:

- The conditions of data protection policies and regulations in the home jurisdiction of the overseas data recipient and their impact on the security of the data export;
- Whether the data protection measures taken by the overseas data recipient satisfy the requirements of Chinese laws, regulations and mandatory standards; and
- The data controller's compliance with Chinese laws, administrative regulations, and ministerial-level rules and regulations.

Step-by-Step Analysis of the Requirements of a Self-Assessment vis-à-vis a CAC Assessment

The provisions of Article 5 of the Measures relate to factors that must be considered in a self-assessment report, while the provisions of Article 8 set forth the factors that will be considered under a CAC Assessment.

1. Lawfulness, Legitimacy & Necessity of Data Export

Both the self-assessment and the CAC Assessment require applicants to explain the lawfulness, legitimacy, and necessity of the purpose, scope, manner, etc. of the data export.[1]

Besides this, for a self-assessment, Article 5(1) requires companies to explain how the data will be processed by the overseas recipient to prove that the processing is lawful, legitimate and necessary.

2. Security of Data Export

Article 5(3) requires the self-assessment report to detail the responsibilities and obligations that the overseas recipient has undertaken to bear and whether its management and technical measures, capabilities, etc. employed for the performance of such responsibilities and obligations can ensure the security of the data exported.

In contrast, Article 8(2) for CAC assessments requires a broader assessment. It focuses on the impact of the data security protection policies and regulations and the cybersecurity environment of the country or region where the overseas recipient is located on the security of the data transferred overseas. It also assesses whether the level of data protection of the overseas recipient satisfies the provisions of the laws and administrative regulations, and the requirements of the mandatory national standards of China.

3. Type of Exported Data & Associated Export Risks

There is substantial overlap in the requirements under Article 5 and Article 8, which both focus on examining the scale, scope, type, and sensitivity of data that will be exported and the risks associated with the proposed data export activities.

The focus of a self-assessment and a CAC Assessment is as follows:

- The scale, scope, type, and sensitivity of the data to be exported and the risks that the data export could pose to national security, the public interest or the lawful rights and interests of individuals or organizations.[2]
- The risk of data being tampered with, damaged, leaked, lost, diverted, or illegally accessed or used, etc. in the course of and after data export, and whether the channels available for safeguarding rights and interests in personal information are unobstructed etc.[3]

4. Draft Legal Document

The requirements under Article 5 and Article 8 also overlap with respect to what applicants must provide for in their legal document, such as a data processing agreement or a data transfer undertaking, with oversea data recipients (Legal Document).

Both assessments ask applicants to explain whether the Legal Document to be concluded fully provides for the responsibilities and obligations for the protection of data security.[4]

5. Other Considerations

Self-assessment reports must also identify any other matters that could affect the security of the data being exported.[5]

CAC Assessments will also examine if the data export activities comply with the laws of the People's Republic of China, administrative regulations, and ministerial-level rules, and regulations over the past two years before the application[6] and any other matters the CAC deems necessary to assess.[7]

Structure of a Self-Assessment Report

According to the Guidelines, a self-assessment report shall include the following four parts:

Part one

Part one must contain a brief description or overview of the self-assessment.

Part two

Part two must detail the particulars of data export activities, including without limitation:

- Basic information about the date controller, including the shareholding structure and ultimate controller, domestic and outbound investment, etc.;
- Business[8] and information system involved in the data export, including data asset, data centers and cloud services involved in the contemplated data export as well as the relevant data links,[9] etc.;
- Information about the data to be exported, including domestic and overseas system platforms and data centers to store data involved and information about the provision of data exported to other recipients;
- Security protection capability of the data controller, such as data protection management and technical capacities, certification of the effectiveness of data security safeguards, etc.;
- Information about the overseas recipient, including information about the data security protection policies and regulations and the cybersecurity environment of the country or region where the overseas recipient is located; and
- Key provisions regarding data export and security protection in the Legal Document.

Parts three and four

In part three, applicants must provide a risk assessment of the contemplated data export activities; and in part four, all necessary conclusions reached from the assessment.

B. DRAFT LEGAL DOCUMENT REQUIREMENT

As noted above, those applying for a CAC Assessment must submit a draft Legal Document with their application. In practice, a data controller and an oversea data recipient should agree on a draft Legal Document before the data controller applies for the CAC Assessment.

Among the six key arrangements required to be included in the Legal Document under the Measures, the following key points may require a local law and enforcement review from the relevant overseas jurisdiction's perspective when the Legal Document is prepared:

- The restrictions on the oversea recipient's retransfer of data exported to other entity or individual;
- The security measures to be adopted by the overseas recipient when there is any material change in the actual control or business scope of the overseas recipient, or when the data security protection policies

and legislation and cybersecurity environment have changed or any other force majeure event has occurred in the country or region where the overseas recipient is located, which makes it difficult to ensure data security; and

- The appropriate emergency response measures and open channels to ensure individuals to uphold their personal information rights and interests in the event of a data breach relating to the data exported.

From the Guidelines, we can tell that the Legal Document does not necessarily have to be a data transfer agreement between a data controller and an overseas data recipient. It could be a commercial contract with data transfer or otherwise processing clauses or an undertaking applicable to the group companies of a multinational company, but the six arrangements regarding the data export and the security protection should be included in such Legal Document.

According to the Guidelines, contractual clauses related to data export in the Legal Document shall be highlighted, circled, or otherwise prominently marked. In terms of the language of the Legal Document, the Chinese version shall prevail. If the Legal Document does not have a Chinese version, a Chinese translation should be provided as well.

C. OTHER REQUIREMENTS FOR AN APPLICATION

The application form for the CAC Assessment implies that both the data controller and the overseas data recipient must have a data protection officer and a management institution, as the form requires both to provide the relevant information on their data protection officers and management institutions.

A data controller may engage a third party to assist it in conducting their self-assessment and compiling a report, according to the Guidelines. However, when they do so, the official chop of the third party must be affixed on the relevant pages of the self-assessment report to certify the authenticity of the content provided by the third party.

TAKEAWAYS

- Because a self-assessment must be conducted within three months before a company applies for a CAC Assessment and because these assessment can be lengthy, companies should prioritize conducting them.
- Companies must disclose their security protection capability in a self-assessment report (e.g., data protection management and technical capacities, certification of the effectiveness of data security safeguards, etc.). Companies should also implement internal measures and policies on data security before applying for a CAC assessment.
- Because a CAC Assessment requires companies to provide an assessment of the data privacy protection systems of the home country or region of an overseas data recipient, companies should seek advice of counsel in the country or region other than China as well when preparing for a CAC Assessment.

In our next alert, we will consider procedures, timeline of a CAC Assessment, circumstances that required a renewal or reapplication of a CAC Assessment, as well as consequences of non-compliance.

FOOTNOTES

[1] *See* Articles 5(1) and 8(1) of Measures for Security Assessment of Data exports.

[2] *See* Articles 5(2), 8(3), and 8(4) of Measures for Security Assessment of Data exports.

[3] *See* Articles 5(4) and 8(3) of Measures for Security Assessment of Data exports.

[4] *See* Article 5(5) and Article 8(5) of Measures for Security Assessment of Data exports.

[5] *See* Art. 5(6) of Measures for Security Assessment of Data exports.

[6] *See* Article 8(6) of Measures for Security Assessment of Data exports and the Guidelines.

[7] *See* Article 8(7) of Measures for Security Assessment of Data exports.

[8] The business involved in the data export shall be consistent with the business under the Legal Document.

[9] The information about the data link that is required to be disclosed to the CAC includes link providers, number and bandwidth of links, names of domestic and overseas data centers, physical location of machine rooms, Internet Protocol addresses, etc.

KEY CONTACTS

AMIGO L. XIE
PARTNER

HONG KONG
+852.2230.3510
AMIGO.XIE@KLGATES.COM

DAN WU
COUNSEL

SHANGHAI
+86.21.2211.2083
DAN.WU@KLGATES.COM

PRUDENCE PANG
ASSOCIATE

HONG KONG
+852.2230.3519
PRUDENCE.PANG@KLGATES.COM

