China Issued Application Guidance for Data Export Security Assessment: Impact on Multinational Business

By Xun Yang | Yuwei Xia | Yara Yang

On late Aug 31st 2022, the Cyberspace Administration of China("**CAC**") promulgated the first edition of the *Application Guidance for Data Export Security Assessment* (the "**Guidance**"). Being released just ahead of the *Assessment Measures of Data Export Security Assessment* (the "**CAC Assessment Measures**") becoming effective, the Guidance provides for the manners, procedures and documentations required for a data export security assessment under the CAC Assessment Measure (the "**CAC Assessment**").

1. Scope of Application

The Guidance defines the scope of data export where CAC Assessment is required.

In consistency with the answers to reports' question during the promulgation of the CAC Assessment Measure, a "data export" is defined to include, among others, the following situations: (1) a data handler transfers, stores, out of the territory of PRC, data which are collected and generated in its operation in PRC, (2) a data handler stores, in the territory of PRC, data it collects and generates, with overseas institutes, organizations or individuals having access to these data or having rights to retrieve, download or output these data. It appears that the scope of "data export" is defined very broad that, as far as data may physically flow outside of China (either in the form of being transferred to an overseas server or of being temporarily viewed by anyone outside of China), such data are considered exported.

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

The Guidance also restates the thresholds by which a data export requires CAC Assessment as provided for under the CAC Assessment Measure. A data handler ("**Data Exporter**") is required to apply for CAC Assessment when (1) it exports important data, (2) the Data Exporter which exports personal information is a critical information infrastructure operator or handles personal information of more than 1 million individuals, (3) the Data Exporter which exports personal information has accumulatively transferred personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals since Jan.1st of the previous year, or (4) other circumstances where CAC Assessment is required by CAC.

Despite the Guidance, some practical issues about CAC Assessment remains unclear. For example, by reading the Guidance, a Data Exporter which possesses personal information of more than 1 million individual customers, needs to undergo the CAC Assessment procedure even when it only exports a small volume of employee information. However, how the volume of customer information saved in China is relevant to the small volume of employee information to be exported? The Guidance addresses no response to this issue.

Another issue yet to be clarified is that, whether hosting data on an overseas cloud constitutes a data export. Arguably, when hosing data on an overseas cloud, there may be no overseas recipient *per se*. In particular, the service provider who provides the cloud space may not have legitimate access to any data stored on the cloud. However, according to the Guidance, that the storage of data on an overseas cloud is still considered a data export. The rationale behind the rule is that CAC may concern that, after data flow outside of China, they may be exposed to risks arising from lack of personal information protection in foreign jurisdictions and to political risks in foreign countries. Thus, according to the Guidance, the geographic location of the servers is one of the factors to be considered during the CAC Assessment.

As such, a data handler who hosts data on an overseas cloud may still be considered a Data Exporter since the cross-border transfer of data will still incur risks and thus need to be regulated. Since there is no "recipient" *per se* during the "data export", the Data Exporter may submit the cloud services contract as the "legal document" under the CAC Assessment Measures, to support the application for CAC Assessment.

2. The CAC Assessment Procedures

In accordance with the Guidance, a Data Exporter must submit application materials in writing together with a corresponding electronic version. The application materials include: (1) photocopy of unified social credit code certificate; (2) photocopy of the identification card of legal representative; (3) photocopy of the identification card of the agent; (4) power of attorney of the agent; (5) Application Form of Data Export Security Assessment; ("**Application Form**") (6) photocopy of contracts relevant to data export and other binding legal documents to be signed between the Data Exporter and the outbound recipients; ("**Legal Documents**") (7) Data Export Risk Self-Assessment Report ("**Self-Assessment Report**") (8) other relevant supporting materials.

The Guidance also mentions that the materials under (6) and (8) could be written in a foreign language, but a Chinese translation thereof must be submitted simultaneously. Surely the translation requirement will increase the administrative burden on multinational companies considering most of the contracts are signed in foreign languages, but this is a requirement which can be satisfied with little difficulties. Additionally, in accordance with Application Form, the terms stipulating the obligations between Data Exporter and the recipient under Art. 9 of CAC Assessment must be clearly labeled in Legal Documents with prominent marks like highlights and frames, which indicates that said terms under Art.9 of CAC Assessment must be clearly incorporated into the Legal Documents, and that said terms will likely be carefully reviewed by CAC.

In respect of procedural requirements, how CAC will proceed with the CAC Assessment remains a mystery. The Guidance makes no hard commitment on the timeline for the CAC Assessment, only stipulating that the Data Exporter will be notified of the estimated time if the time for the CAC Assessment is extended from 45 days.

The Guidance does not set out a specific procedure for the examination under the CAC Assessment. It does not mention any consultation with other government bodies nor does it indicate an onsite inspection. It appears that the CAC Assessment is primarily based on review of documentations. As indicated in Art. 10 of the CAC Assessment Measure, CAC will likely involve technical testing institution for the assessment from a technical aspect; and consult relevant sectorial regulator from a regulatory aspect.

According to the template application documents provided for under the Guidance, it appears that the CAC Assessment pays much attention to the data security management capability of both the Data Exporter and of the outbound recipient. For example, in the template of Self-Assessment Report, the Data Exporter is required to demonstrate the reliability of its IT infrastructure including the IT systems, data center, communication links relevant to data export, as well as the systems platform and data centers to which the data are exported. In addition, a Data Exporter is required to submit a validity certificate for its data security protective measures such as the data security risk assessment, data security ability certificate, data security inspection and evaluation, data security compliance audit or cyber security level protection evaluation. It is worth noting that, in order to further confirm the authenticity and reliability of the Self-Assessment Report, the CAC requires that the third-party institution which performs the self-assessment endorses the content contained in the Self-Assessment Report by chopping its official seal on it. In other words, the party which participates in completing the Self-Assessment Report must disclose its name and take corresponding responsibility for its opinions.

3. Substantive Requirements

The performance of CAC Assessment is a comprehensive review of data and cyber security law compliance by the Data Exporter. Under the Guidance, CAC requires that, during the CAC Assessment, the compliance by the Data Exporter with data and cyber security laws be taken into account in assessing the data export risks, including the compliance history, individual responsibility and the managerial and technical mechanism of the Data Exporter. In particular,

- Under the Application Form, the Data Exporter must disclose its compliance history, including any administrative penalty it receives, any investigation conducted by relevant competent regulatory authorities during its business operations and its rectification, with a focus on area of data and cyber security in the past 2 years.

- The Data Exporter must disclose the data security officer and the management body of Data Exporter and of the overseas recipient, including the names, contacts, occupations, nationalities, identifications numbers.

- The Data Exporter must elaborate its data protection management system, including life-circle management, classification, contingency plan, risk assessment, and personal information interest protection mechanism. Additionally, the Data Exporter is required to introduce its technical measures adopted to protect data at all stages, including collection, storage, use, process, transmission, provision, disclosure, deletion, etc.

This essentially means that the compliance with data and cyber security laws is an important element in passing the CAC Assessment.

4. Practical Suggestions

CAC Assessment Measures have officially come into effect yesterday. The Guidance and the public consultation hotline were subsequently published. For multinational companies which routinely exports data, the CAC Assessment is an inevitable burden.

Obviously, to continue the existing data exports and to go through CAC Assessment as required means a significant administrative burden for multinational companies. Consequently, a few multinational companies are adopting a China for China policy by moving its regional data base to China to reduce the frequency and volume of data exports.

It is recognized that multinational companies may still need to export certain data for global process. In this case, it would be advisable to shall set up the internal data export risk assessment procedures as soon as possible, by taking into the “template of Self-Assessment Report” under the Guidance. It would effectively reduce the administrative cost to build the risk assessment procedure, as a standard process, into the internal management procedure.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli,
Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road,
Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD