THE CAC ASSESSMENT COLLECTION – PART 1: WHAT YOU SHOULD CONSIDER BEFORE EXPORTING DATA FROM CHINA

Date: 6 December 2022

China Data Protection, Privacy, and Security Alert

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

With the rapid development of the global digital economy, multinational companies (MNCs) have been forced to find legally compliant ways to transfer data across borders. In the past, many MNCs relied on data transfer agreements that incorporated standard contractual clauses (SCCs) (e.g., standardized and pre-approved model data protection clauses) that allow controllers and processors to comply with the *General Data Protection Regulation*[1] when transferring personal data within and outside of the European Economic Area. Until September 2022, this was the generally accepted practice to ensure compliance when transferring data to and from the People's Republic of China (PRC or China).

However, after the Cyberspace Administration of China (CAC) promulgated the *Measures for Security Assessment of Data exports* (Measures) (effective since 1 September 2022), MNCs can no longer automatically rely on data transfer agreements as a compliance panacea when exporting data to and from China. Rather, MNCs must now assess and determine first if their data exporting activities from China are subject to a security assessment conducted by the CAC under the Measures (CAC Assessment).[2]

The Measures stipulate in greater detail the thresholds, application documents, conditions and procedures for a CAC Assessment that are required for exporting data from China, which have been generally addressed under the *Cybersecurity Law*, the *Data Security Law*, and the Personal Information Protection Law (PIPL),[3] three laws that form China's data governance regime.

Late on 31 August 2022, the night before the Measures took effect, the CAC issued the *Guidelines on Application of Security Assessment of Data exports (First Version)* (Guidelines). The Guidelines provided more concrete and practical guidance, identifying data export activities that are subject to the CAC Assessment, clarifying the extent to which an applicant must conduct a self-assessment before applying for a CAC Assessment, and detailing which applications and supporting documents must be filed to receive a CAC Assessment approval.

Among four routes to legitimize data export from China,[4] the CAC Assessment is mandatory and can exclude the use of other routes. Given that a standard CAC Assessment could take up to 57 business days to complete, data controllers[5] who are subject to the CAC Assessment route should act immediately to prepare and submit their applications now to avoid being prohibited from exporting data from China.

This series of alerts will discuss key concepts and requirements of the CAC Assessment, as well as recommended actions to be taken by MNCs.

In Part 1, we will delve into a key question – what data export activities must undergo a CAC Assessment. In Part 2, we will take a deeper look at what must be done before applying for a CAC Assessment. In Part 3, we will examine procedures, timeline, renewal, and reapplication of a CAC Assessment, as well as consequences of non-compliance.

WHAT ARE DATA EXPORT ACTIVITIES UNDER THE MEASURES?

The Measures stop short of defining "data export." Instead, the Guidelines mostly confirm comments made by CAC officers at a 7 July 2022 press conference, which can be summarized as defining "data export" as encompassing the following activities:

- A data controller that transfers any data collected and generated in its operation within the territory of China to an overseas recipient or stores such data in an overseas recipient;
- A data controller that stores within the territory of China any data it collects and generates with any overseas entity, organization, or individual having access to, retrieving, downloading, or outputting such data; or
- Other behaviors of data export prescribed by the CAC.

In terms of the definition of a "data export activity," below are key differences between Article 1 of the Guidelines and the draft national guideline – *Information Security Technology – Guidelines for Data Export Security Assessment (Draft for Consultation)* (TC260 Draft Guidelines) proposed by the National Information Security Standardization Technical Committee (SAC/TC260) in 2017.

1. The Scope of "Data" Under the Guidelines is Not Limited to Data Collected and Generated by a Data Controller in Its Operations Within the Territory of China (China Operations Data).

Under both the Guideline and the TC260 Draft Guideline, if a data controller is deemed to produce or handle China Operations Data, export of such China Operations Data from China is a "data export activity."

According to the TC260 Draft Guidelines, in the event that a China-registered data controller only conducts business, provides goods or services to overseas institutions, organizations, or individuals, and does not involve the personal information of China domestic citizens or important data in China, data collected or generated by it under the foregoing circumstances will not be considered China Operations Data. Accordingly, export of such data from China is not a data export activity under the TC260 Draft Guidelines.[6]

However, the Guidelines appear to extend the applicability of a CAC Assessment to data that is not China Operations Data but is stored in China when a foreign entity or individual can access the data. As long as such data is stored within the territory of China, regardless of where it is collected or generated, access to such data by a foreign entity or individual will be deemed as a data export activity under the Measures.

Thus, the applicability of the CAC Assessment in this regard is very broad, especially in instances when data does not relate to nor is relevant with any data collected or generated in or from China.

2. Is Access to Data Stored in China by a Foreigner Who is Located in China a Data export Activity Under the Measure?

Under Article 3.7 of the TC260 Draft Guidelines, when foreigners who are located within the territory of China can access data stored in China, it will be considered a data export activity (e.g., when China Operations Data is provided to a foreign journalist who is in China).

It is unclear if such a scenario is a data export activity under the Measure and the Guidelines.

If this scenario is covered by the Measures, provision of important data by any data controller or provision of personal information by certain data controllers to a foreigner who is located in China could trigger a CAC Assessment as well. This point needs to be further clarified in practice.

WHAT TYPES OF DATA EXPORT ACTIVITIES MUST UNDERGO A CAC ASSESSMENT?

In the event that a data transfer is a data export activity covered by the Measures, export of important data or certain data controllers' export of personal information will trigger a CAC Assessment.

Article 4 of the Measures require the following five types of data export activities to go through a CAC Assessment. Given the low threshold and broad coverage of these types of data export activities, it appears that most data export activities by MNCs could trigger the CAC Assessment.

1. Export of Important Data

What is "Important Data"?

The concept of "important data" was first introduced into the law in 2017 by Article 37 of the Cybersecurity Law. It requires critical information infrastructure operators (CIIO) to store in China personal information and important data which are collected and produced during their operations within the territory of China.

The Data Security Law further provides that China shall implement a classified and graded data protection system and catalogues of important data shall be formulated. It requires each regional government and central governmental or regulatory department to determine the specific catalogue of important data for their respective region and department, and in relevant industries and areas.[7]

However, neither the Cybersecurity Law nor the Data Security Law defines "important data." No official catalogue of important data has been promulgated yet either.[8]

A generic definition of "important data" is stipulated in the Measures as "any data, the tampering, damage, leakage, or illegal acquisition or use of which, if it happens, may endanger national security, the operation of the economy, social stability, public health, and security, etc."[9]

On 14 September 2022, SAC/TC260 released the *Information Security Technology – Requirements for Classification and Grading of Network Data (Draft for Comments)* for public comments by 13 November 2022. Once this national standard becomes effective, various localities and governmental or regulatory departments can carry out data classification and grading activities with reference to this standard, and important date would be identified accordingly.

In its local guidelines on application for the CAC Assessment, the Jiangsu office of the CAC listed seven catalogues of important data with reference to the list of important data in the *Regulations on Network Data Security Management (Draft for Comments)* promulgated by the CAC on 14 November 2021. This could be a practical solution to determine the scope of important data before the official catalogues of important data are available.

2. Export of Personal Information by a CIIO

How to Know Whether You Are a CIIO?

According to *Regulations on the Security Protection of Critical Information Infrastructure*, a CIIO will be designated by the government authorities and will be notified about the designation.[10]

3. Export of Personal Information by a Personal Information Handler Who Processes the Personal Information of More Than 1 Million People

What is "Personal Information"?

"Personal information" is defined in the PIPL as any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized.

Appendix A to *National Standard of Information Security Technology – Personal Information Security Specification* (PIS Specification) provides 13 categories of personal information as examples for reference.

4. Export of Personal Information by a Personal Information Handler Who Has Exported the Personal Information of 100,000 People Cumulatively or the Sensitive Personal Information of 10,000 People Cumulatively Since 1 January of the Previous Year

What is "Sensitive Personal Information"?

"Sensitive personal information" is defined in the PIPL as personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health, financial account, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14.

Appendix B to PIS Specification provides five categories of personal information as examples for reference.

5. Other Circumstances Where an Application for the CAC Assessment is Required as Prescribed by the CAC

Such other circumstances are subject to further clarification of the CAC in practice in the future.

CONCLUSION

If companies assume they can simply export data from China based on a data transfer agreement it could be very problematic. Before a data transfer, it is important to conduct a data mapping of data provision, sharing, or other transfer activities from or in China and assess whether such activities are data export activities under the Measures, and, if so, whether such data export triggers a CAC Assessment.

In our next alert, we will be considering what companies must do before they can apply for a CAC Assessment.

FOOTNOTES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] A consultation paper on the Chinese SCCs was issued by CAC on 30 June 2022. Hopefully, the official version of the Chinese SCCs will be available by the end of 2022.

[3] Article 37 of the Cybersecurity Law, Article 31 of the Data Security Law and Article 40 of the Personal Information Protection Law respectively require a CAC assessment for export of important data or personal information by a critical information infrastructure operator (CIIO). Article 31 of the Data Security Law further expands this requirement to important data export by non-CIIO data handlers. Article 40 of Personal Information Protection Law requires the CAC Assessment for non-CIIO personal information handlers who process personal information that reaches the threshold amount prescribed by the CAC.

[4] Under Article 38 of the Personal Information Protection Law and Article 35 of the Online Data Security Management Regulations (Draft for Comment), the four routes are: (1) CAC Assessment, (2) Certification (PRC compliant binding corporate rules), (3) PRC compliant SCCs and (4) other route prescribed by law, administrative regulations or the CAC. Please see our client alert on the certification: https://www.klgates.com/What-You-Need-to-Know-About-China-Binding-Corporate-Rules-Under-the-New-Certification-Specifications-7-22-2022.

[5] The China data governance system does not contain separate definitions of a data controller and a data processor. The definition used is a "data handler" and a data processing contractor. A data handler, by definition, is a data controller.

[6] The TC260 Draft Guidelines defined "China Operations" in Article 3.2. It means a network operator conducts business and provides products or services within the territory of China. Data that is not collected or generated in China Operations is not China Operations Data, according to the TC260 Draft Guidelines. Indicators for determining whether a network operator conducts business in the territory of China, or provides products or services to China, include but are not limited to: using Chinese language; using RMB as the settlement currency; delivering logistics to China, etc. See note 1 to Article 3.2 of the Draft Guidelines. Under the TC260 Draft Guidelines, the following examples are NOT data export because data involved is not "China Operations Data":

(a) Personal information and important data that are not collected and generated in domestic operations are exported through China without any modification or processing; and (see Note 2 to Article 3.7).

(b) Personal information and important data that are not collected and generated in domestic operations but stored and processed in China before leaving China, and the data export does not involve any personal information and important data collected and generated during domestic operations. (see Note 3 to Article 3.7).

[7] Please refer to our alert about the Data Security Law for more details: https://www.klgates.com/Chinas-New-Data-Security-Law-Bolsters-Its-Data-Security-Legal-Regime-7-9-2021.

[8] *Several Provisions on Vehicle Data Security Management (for Trial Implementation)*, effective on 1 October 2021, defines "important data" and lists six catalogues of important data in the vehicle sector. In addition, Appendix A to the TC260 Draft Guidelines provides a detailed catalogue of important data across 27 different

industry sectors.

[9] See Article 19 of Measures for Security Assessment of Data exports.

[10] Please refer to our alert about CIIO for more details: https://www.klgates.com/Overview-of-the-New-Implementing-Rules-on-Critical-Information-Infrastructure-in-China-and-Key-Takeaways-10-19-2021.

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

