DEACONS
的近律師行

Corporate Commercial Client Alert

China Trade & Investment

21 July 2022

The Measures for the Security Assessment of Outbound Data promulgated officially

Edwarde Webre and Minning Wei

The Cyberspace Administration of China ("CAC") promulgated the *Measures for the Security Assessment of Outbound Data* (the "Measures") on 7 July 2022, which will come into effect on 1 September 2022. Compared to the third draft of the Measures (the "Draft") released in October 2021, the provisions under the Measures are more specific and developed and can be more practicably applied.

Scope of application

The Measures are applicable to the security assessment of important data and personal information ("PI") collected/generated in domestic operations within China that are transferred abroad by a data processor. "Important data" is defined broadly to be "the data that may endanger national security, economic operation, social stability, public health and security, etc. once they are tampered with, damaged, disclosed, illegally obtained or illegally used, etc."

Risk self-assessment

The Draft required a data processor to conduct a risk self-assessment before transferring any data abroad, which has been revised under the Measures to provide that a risk self-assessment shall be conducted before a data processor applies to the CAC for a security assessment of the outbound data. The Measures do not clarify whether data processors that are not required to apply for the security assessment need to conduct a risk self-assessment. To be prudent, it is advisable that all the data processors in Mainland China conduct a risk self-assessment in accordance with the Measures before they transfer the data abroad, regardless of whether a security assessment is required.

With regard to the key risk self-assessment items under the Draft, the item of "whether the management, technical measures and capabilities of the data processor in the data transfer link can prevent data leakage, damage and other risks" has been deleted. A general miscellaneous provision that "any other item(s) that may affect the security of outbound data" is added instead. "The relevant contract(s) for the outbound data concluded with the overseas recipient(s)" under the Draft has been expanded to "contracts or other documents with legal effect". The key assessment items of risk self-assessment are as follows:-

1. the legality, justifiability, necessity of the outbound data transfer and the purpose, scope and method of the overseas recipient's data processing;

2. the scale, scope, type and sensitivity of the outbound data; risks to national security, public interests and the legitimate rights and interests of individuals or organisations that may arise from the outbound data transfer;

3. the responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management, technical measures and ability to perform the responsibilities and obligations can ensure the security of the outbound data;

4. risks of tampering, damage, leakage, lost, transfer or illegally obtained, illegally used, etc. when the data are being transmitted and after they have been transmitted abroad, and whether the channels for individuals to maintain their rights and interests in personal information are unblocked;

5. whether the relevant contract(s) or other document(s) with legal effect (together referred to as "Legal Document(s)") for the outbound data to be concluded with the overseas recipient(s) fully specifies the responsibilities and obligations for data security protection; and

6. any other item(s) that may affect the security of outbound data.

The specific requirements of the Legal Document(s) to be concluded with the overseas recipient(s) under the Measures are similar to the relevant contracts required under the Draft subject to some adjustment.

Security assessment of outbound data by the CAC

The circumstances that will trigger the CAC's security assessment are revised in the Measures. A data processor shall apply to the CAC for security assessment of outbound data through the provincial cyberspace administration where it is located in any of the following circumstances:-

1. a data processor provides important data abroad;

2. any critical information infrastructure or any data processor that process PI of more than 1 million people provides PI abroad;

3. any data processor provides the PI of more than 100,000 people to overseas or sensitive PI of 10,000 people accumulatively since 1 January of the previous year;

4. any other circumstances that require security assessment as determined by the CAC.

The procedures of the security assessment by CAC are specified under the Measures:-

1. a data processor shall conduct risk self-assessment.

2. a data processor that applies for the security assessment shall prepare application documents as required and submit the same to its local provincial cyberspace administration.

3. the provincial cyberspace administration shall check the completeness of the application documents within 5 working days from the receipt of the application and shall pass the application to the CAC if the documents are complete. Otherwise, it shall return the application documents to the data processor and inform it of the documents required to be supplemented.

4. the CAC shall determine whether to accept the application and notify the data processor in writing within 7 working days upon the receipt of application from the provincial cyberspace administration.

5. the CAC shall complete the security assessment within 45 working days of the issuance of acceptance notice to the data processor. In a case that is complicated or any documents need to be supplemented or revised, the CAC may extend the assessment period appropriately and inform the data processor of the estimated period of time.

It is worth noting that the Draft provision limiting the CAC's review extension to "no longer than 60 working days in general" has been deleted. As such, the data processor may need to reserve more time for the security assessment in practice.

A new article regarding re-assessment has been inserted into the Measures, providing that if a data processor has any objection to the assessment result of the CAC, it may apply for a re-assessment to the CAC within 15 working days upon the receipt of the assessment result. The result of the re-assessment shall be final.

Under the Measures, the effective term of the security assessment is 2 years starting from the date of the issuance of the assessment result. Compared with the Draft, the circumstances under which a re-assessment needs to be made has been adjusted in the following two aspects:-

1. under the Measures, the re-assessment is required only when the change to the purpose, method, scope or category of outbound data or to the usage or method of data processing by the overseas recipient has impact on the security of the outbound data. In the Draft, the assessment is required to be made again if any change occurs.

2. the Measures also require re-assessment not only when there is any change that may affect the security of the outbound data in the legal environment of the country or region where the overseas recipient is located, but also if there is a change in the policies and regulations of data protection and the cyber security environment there and when there is any event of force majeure. “Any change in the contract(s) between the data processor and the overseas recipient” in the Draft has been revised to “any change in the Legal Document(s) between the data processor and the overseas recipient”.

The requirement that “data outbound activities shall cease if the re-assessment has not been done as legally required” which appeared in the Draft has been deleted. Instead, the Measures provide that “where the CAC finds that the security of any outbound data which has passed the assessment no longer meets the security management requirements in the actual process, it shall notify the data processor in writing to terminate the outbound data activities. The data processor concerned shall make rectification as required and complete the re-assessment if it intends to continue its outbound data activities.” Therefore, if a data processor encounters any circumstances that require re-assessment, it is advisable for it to apply for re-assessment as soon as possible to avoid any adverse impact on the data outbound activities.

Suggestions

The Measures will come into effect on 1 September 2022. Any data outbound activity incompliance with the Measures before it is effective shall be rectified within 6 months upon the effective date, i.e., by 28 February 2023. The data processors in China shall review and adjust its data outbound activities as required by the Measures and take necessary actions for compliance within the stipulated time.

Further, the data processors shall keep a close eye on the implementation and interpretation of the Measures by the CAC afterwards and update its risk self-assessment periodically for continuous compliance.

Want to know more?

Cynthia Chung
Partner
cynthia.chung@deacons.com
+852 2825 9297

Machiuanna Chu
Partner
machiuanna.chu@deacons.com
+852 2825 9630

Edwarde Webre
Partner
edwarde.webre@deacons.com
+852 2825 9730

Elsie Chan
Partner
elsie.chan@deacons.com
+852 2825 9604

Helen Liao
Partner
helen.liao@deacons.com
+852 2825 9779

Stefano Mariani
Partner
stefano.mariani@deacons.com
+852 2825 9314