Baker McKenzie FenXun.

Client Alert

July 2022

The Clock is Ticking! - Cyberspace Administration of China Finalizes Measures for Security Assessment of Transfers of Data Abroad

In brief

Just one week following the release of the draft *Rules concerning the Standard Contract for Cross-Border Transfers of Personal Information* ("**Draft China SCCs Rules**") (see our prior client alert), the Cyberspace Administration of China (CAC) finalized and issued the long-awaited *Measures for the Security Assessment of Transfers of Data Abroad* ("**Measures**") on 7 July 2022. The Measures provide the implementation rules and guidelines concerning the security assessment mechanism for cross-border data transfers (**CBDT**) outside of China, as established in China's three overarching data protection laws, the *Cybersecurity Law* (CSL), the *Data Security Law* (DSL) and the *Personal Information Protection Law* (PIPL). The Measures will take effect and will be implemented from 1 September 2022. Companies will have a grace period of six months to comply with the Measures.

In this issue

Circumstances and Thresholds Triggering CBDT Security Assessment

Article 4 of the Measures provides that a security assessment administered by CAC will be required for transferring data outside of China if any of the following conditions is fulfilled:

(i) provision of "important data" abroad;

(ii) provision of personal information abroad by a critical information infrastructure operator (CIIO) or a personal information processor (PIP, as defined under the PIPL, a term akin to a "data controller" under the EU General Data Protection Regulation) that processes personal information of not less than 1 million individuals;

(iii) provision of personal information of more than 100,000 individuals in aggregate abroad or sensitive personal information of more than 10,000 individuals in aggregate abroad since 1 January of the preceding calendar year; and

(iv) other circumstances where the CAC requires the filing of an application for security assessment for provision of data abroad.

It is worth noting that CAC has clarified in its Q&As concerning the Measures that, in addition to transferring data abroad, remote access from a foreign jurisdiction to personal information and important data stored within China in a cross-border manner will also constitute "providing data abroad" and the relevant CBDT requirements will apply.

Another important point to note is that there is no quantitative threshold for the security assessment in terms of providing important data abroad. So, technically speaking, a data exporter providing any amount of important data abroad will be subject to the CBDT security assessment. The Measures define "important data" as *"any data that, once altered without authorization, destroyed, leaked, obtained illegally or used illegally, could jeopardize national security, economic operation, public health and safety, etc.,*" which is generally in line with the definitions of important data proposed in a number of draft rules and recommended national standards, such as the draft *Cyber Data Security Regulations* and the *Guidelines for Identification of Key Data*. As this definition of important data in the Measures is rather general, companies will need to consider said rules and recommended national standards (once they are finalized), as well as the industry and sector specific legislations and rules to determine and identify the scope of important data relevant to their data processing activities and the CBDT security assessment requirements applicable to them.

Although it is not explicit in any of the underlying legislations and the Measures, the individuals referred to in the conditions listed in the Measures for determining the application of the CBDT security assessment are commonly understood to mean individuals residing in China. It is implied from the draft guidelines concerning CBDT security assessment published in 2018 that personal information collected from outside China and transferred to China for processing without the personal information being combined with any personal information collected or originating in China before being re-exported should not be counted as personal information being transferred abroad for the CBDT security assessment purpose.

As illustrated in the table below, both the Measures and the Draft China SCCs Rules refer to the same number of individuals whose personal information is processed in China or transferred abroad (1 million, 100,000 and 10,000) as the quantitative thresholds triggering the application or non-application of the CBDT security assessment and the China SCCs. Therefore, the CBDT security assessment requirements and the China SCCs requirements are intended to be complementary to each other in terms of regulating CBDT.

All of the following conditions must be concurrently fulfilled to be eligible to use the China SCCs for provision of personal information abroad	**If any of the following conditions is fulfilled, the CBDT security assessment by CAC will be required for the provision of important data and personal information abroad**
	Export of important data (no quantitative threshold) by any company in China
Exporter of personal information (no quantitative threshold) is not a CIIO	Export of any personal information (no quantitative threshold) by a CIIO or
Exporter of personal information processes personal information of less than 1 million individuals residing in China	A PIP processing personal information of 1 million or more individuals residing in China (Large-Scale PIP)
Since 1 January of the previous calendar year, a PIP provides personal information of fewer than 100,000 individuals residing in China to a foreign jurisdiction	Since 1 January of the previous calendar year, a PIP (who is not a CIIO or a Large-Scale PIP) provides personal information of 100,000 or more individuals residing in China OR sensitive personal information of 10,000 or more individuals residing in China to a foreign jurisdiction
Since 1 January of the previous calendar year, a PIP transfers sensitive personal information of fewer than 10,000 individuals residing in China to a foreign jurisdiction	

However, how the quantitative thresholds should be calculated and applied are not crystal clear under the Measures. While the Measures do not specify if the quantitative thresholds should be applied on a legal entity basis, the commonly accepted understanding is that the number of individuals whose personal information is being processed or exported should be calculated on the basis of each legal entity instead of each IT system / application, data flow, use case or business line. Further, where the same legal entity in China transfers the same individual's personal information to multiple overseas recipients (such as affiliates and vendors), it is not entirely clear if the same individual residing in China should be counted only once or be multiplied by the number of overseas recipients receiving such individual's personal information, although it is reasonable to take the view that the same individual whose personal information is exported by the same legal entity in China should be counted only once.

For companies domiciled outside China that directly collect and process personal information of individuals residing in China in a cross-border manner and are thus subject to the extraterritorial application of the PIPL pursuant to Article 3.2 of the PIPL, would the CBDT security assessment mechanism be applicable? This is one of the most frequently asked questions since CAC published the draft version of the Measures in 2021. The final version of the Measures do not provide a clear answer to this question. We take the view that the CBDT security assessment administered by CAC should not be applicable to non-Chinese PIP collecting personal information in a cross-border manner without the involvement of any PIP or entrusted party within China as the exporter of the relevant personal information to such non-Chinese PIP. This is because in such scenario, no legal entity located in China (other than the relevant data subjects whose personal information is directly collected by the non-Chinese PIP) is providing personal information abroad and the non-Chinese PIP, being a data recipient, is not receiving personal information from an exporting PIP in China.

CBDT Security Assessment and Data Localization

One may ask about the interplay between the CBDT security assessment mechanism and the data localization requirement stipulated under the PIPL. Would a legal entity that processes or exports personal information of individuals in an amount above the quantitative thresholds be required to store the relevant personal information locally within China?

According to the CSL, the DSL and the PIPL, data localization requirements are applicable if (i) a PIP is identified by the relevant industry regulator to operate a critical information infrastructure (CII) so that it becomes a CIIO, (ii) a PIP processes personal information above the statutory threshold(s) ("**Large-Scale PIP**"), or (iii) a PIP processes specific types of personal information and is thus subject to industry-specific data localization requirements (such as healthcare, mapping, and financial sector). Although the PIPL does not explicitly state that the threshold to determine a Large-Scale PIP is 1 million individuals residing in China, as this quantitative threshold is mentioned in both the Measures and the Draft China SCCs Rules, it has become quite certain that the 1 million individual-threshold for the CBDT security assessment will also be the threshold to determine a Large-Scale PIP who needs to store within China all personal information it collects and generates in China.

The quantitative thresholds of personal information of more than 100,000 individuals and sensitive personal information of more than 10,000 individuals are premised on a legal entity's act of providing personal information abroad, instead of its act of processing personal information within the China territory (which is what Article 40 of the PIPL refers to as the basis for data localization requirement). Although it is not explicit in the Measures, it is reasonable to believe that crossing these quantitative thresholds alone should not trigger the data localization requirements for the relevant legal entity providing personal information abroad. According to the Measures, however, once the security assessment is triggered, no export of personal information can be conducted unless and until the data exporter has passed the security assessment. That being said, since it will take at least 57 working days to complete the security assessment process for any newly-initiated transfer of personal information abroad by a legal entity located in China, effectively there will be a "standstill" period where personal information to be provided abroad will need to be stored temporarily in China pending the CAC's security assessment result. Such temporary storage of personal information within China during the waiting period would inevitably lead to the need to make use of a local server or database within China by the data exporter, which would operate as a temporary data localization arrangement during such waiting period.

Documentation requirements for CBDT Security Assessment

The Measures require data exporters to submit the following documents in order to apply for a CBDT security assessment:

(a) an application letter;

(b) a CBDT security self-assessment report outlining the risks of transfers of data abroad;

(c) the Legal Document (as defined below) to be concluded between the data exporter and the overseas recipient; and

(d) other documents required for the security assessment by the CAC.

The format for item (a), the application letter, has not been clarified by the CAC.

For the security self-assessment report, Article 5 of the Measures stipulates that the following focus areas should be covered in the self-assessment, which will need to be addressed in the report:

(1) the legality, appropriateness and necessity of the purpose, scope and manner, etc. of the transfer of data abroad and of the processing of the data by the overseas recipient;

(2) the scale, scope, type and sensitivity of the data to be provided abroad, and the risks that the transfer of data abroad could pose to national security, the public interest and the legitimate rights and interests of individuals or organizations;

(3) the responsibilities and obligations that the overseas recipient undertakes to bear and issues as to whether such recipient's management and technical measures and capabilities, etc. in respect of the performance of such responsibilities and obligations can ensure the security of the cross-border data transfer;

(4) the risk of data being exposed to unauthorized alteration, damage. leakage, loss, diversion or being illegally obtained or illegally utilized, etc. during and following the cross-border transfer, and issues as to whether the individuals will have easy access to channels in which they can safeguard their rights and interests;

(5) whether the contract to be concluded with the overseas recipient in connection with the CBDT or other document with legal effect ("**Legal Document**") adequately stipulate the responsibilities and obligations in respect of data security protection;

(6) other matters that may have an impact on security of the CBDT.

The security self-assessment, which is by nature a transfer impact assessment, covers matters that are much broader than those covered in the personal information impact assessment for CBDT required by the PIPL and proposed in the Draft China SCCs Rules. Conceivably, the security self-assessment will inevitably involve the assistance and inputs from the overseas recipient(s), and therefore, could be a time-consuming process.

The Measures do not impose any specific templates or standard clauses to be used for the Legal Document to be submitted for the CBDT security assessment. Instead, Article 9 of the Measures provides that the following should at least be addressed in the Legal Document:

(1) the purpose and method of the provision of data abroad, the scope of the data to be transferred, and the purpose, method, etc. of the processing of the data by the overseas recipient;

(2) the location and duration of retention of the data outside China, and the way in which the data will be dealt with after the retention period has expired, the agreed-upon objective has been achieved or the Legal Document has expired;

(3) binding requirements concerning further transfers of the transferred data by the overseas recipient to other organizations or individuals;

(4) the security measures to be taken by the overseas recipient under certain circumstances (e.g., change of control, change of law, etc.);

(5) the remedial measures and liability for breach of the data security protection obligations, and dispute resolution method; and

(6) the mechanism to deal with data leakage incidents and to ensure data subjects safeguard their rights.

Many of these compulsory provisions are similar to those proposed in the draft China SCCs, so it seems that a data exporter and an overseas recipient may choose to adopt the China SCCs as the basis for the Legal Document. However, unlike the Draft China SCCs Rules, the Measures do not require that the Legal Document must be the only document that controls the CBDT from the data exporter to the overseas recipient, which may give the parties some flexibility to agree on or refer to more elaborate protocols applicable to the CBDT between them. This also means that multinational companies (MNCs) may choose to rely on the China supplementary agreement to its intra-group transfer agreement or the China supplements to the binding corporate rules (BCRs) as the Legal Document for purposes of the CBDT security assessment. It is worth noting that the CAC has the discretion to request for "other documents required for security assessment" under item (d). Data exporters should therefore be mindful when making references to other documents in the Legal Documents to be concluded with the overseas recipient(s) and should be prepared to submit them to the CAC upon request.

There are two technical issues that require the CAC's clarification ahead of the implementation of the Measures: (a) whether a security assessment application may be filed in respect of specific CBDT flow(s), use case, business purpose and/or overseas recipient, or whether the security assessment application must be submitted by a data exporter covering all of its CBDT activities in the same application, and (b) who will be considered as the overseas recipient – must it be the overseas party directly receiving the data being transferred or can the data exporter designate the overseas parent company or affiliate who will engage the various overseas vendors and solution providers as the overseas recipient?

Procedures and Timelines of CBDT Security Assessment

From a procedural perspective, a data exporter needs to carry out a security self-assessment and conclude the Legal Document before the application to the provincial office of the CAC (where the data exporter is located) for the CBDT security assessment. The provincial CAC will conduct a brief review to ascertain if the application materials submitted are complete, and if so, the provincial CAC will pass the application to the central CAC for substantive review. The central CAC will then decide whether to accept the application. Once the application is officially accepted, the central CAC needs to conclude the assessment and make the decision within 45 working days from its acceptance date, which period can be extended for complex cases.

A detailed diagram illustrating the entire process of the CBDT security assessment is attached at the end of this alert for ease of understanding. It is worth noting that the Measures provide for an appeal process. If a data exporter applying for the CBDT security assessment objects to the assessment result made by the CAC, it can apply to the central CAC for re-assessment within 15 working days after receipt of the assessment result. According to the Measures, the re-assessment result is conclusive.

In an uncontested case, the entire security assessment process will take at least 57 working days (which will effectively be around three months), and the timeline may be prolonged if the application is complex or extension is deemed necessary by the CAC. Strictly speaking, no CBDT can be conducted by a data exporter unless and until it has passed the security assessment conducted by the CAC. With this relatively long process, the time it takes to conduct the security self-assessment and the preparation of the application documents, a data exporter would need to budget four months at the very least to complete the entire CBDT security assessment process, and during this time period, a contingent plan to minimize the impact on the relevant business activities requiring CBDT would be necessary.

Key Considerations of CAC in Conducting CBDT Security Assessment

In conducting the security assessment under Article 8 of the Measures, the CAC will review whether the CBDT activities (a) are legitimate, appropriate and necessary and (b) whether they pose a risk to national security, the public interest and the legitimate rights and interests of individuals and organizations, which include the following aspects:

(1) the legality, legitimacy and necessity of the purpose, scope and manner of the CBDT;

(2) the impact that the data security protection policies, laws and regulations, and the cybersecurity environment of the destination jurisdiction will have on the security of data to be transferred abroad; and the issue of whether the level of the data protection provided by the recipient meets the requirements of Chinese laws;

(3) the scale, scope, type and sensitivity of the data to be transferred abroad, and the risk of unauthorized alteration, damage, loss, diversion, illegal access, illegal use, etc. during or after the CBDT;

(4) whether data security and the rights and interests in the personal information can be fully and effectively protected;

(5) whether the Legal Documents to be concluded between the data exporter and the overseas recipient adequately provides for the responsibilities and obligations in respect of data security protection;

(6) compliance with the laws, administrative regulations and ministry-level regulations of China; and

(7) other matters that the central CAC deems necessary.

These focus areas are more or less the same as those to be addressed in the security self-assessment and the Legal Document. Therefore, a robust and sufficiently-elaborate self-assessment report and a Legal Document sufficiently addressing the mandatory matters concerning the intended CBDT would be critical. In particular, the data processor needs to give careful consideration and prepare a robust analysis concerning the legality (i.e., whether the informed consent requirement for CBDT has been complied with), the appropriateness (i.e., data minimization and direct relevance of CBDT for the relevant business needs / objectives) and the necessity (the business / operational reasons to justify the intended CBDT) in the self-assessment report.

Validity Period of CBDT Security Assessment Results

The result of the CBDT security assessment issued by the CAC has a validity period of two years, which shall start from the date of issuance of the assessment result. During the validity period, a data exporter will need to apply for a re-assessment in the event of: (i) any change of the purpose, method, scope or type of the transfer or the purpose or manner of the overseas recipient's processing, which may affect the security of the transferred data; (ii) data will be retained outside China for a period longer than was previously cleared in the security assessment by the CAC; (iii) any change of the data protection laws / policies or cybersecurity environment of the destination jurisdiction, force majeure events, change of actual control of the data exporter or overseas recipient, or change of the Legal Document, which may affect the security of the transferred data; and (iv) other situations that may affect the security of the transferred data.

It is unclear under the Measures whether, in the above scenarios, the entire security assessment process must be re-initiated or a simplified process will be applicable. Also, how this re-assessment would impact the data exporter's ongoing CBDT remains to be ironed out by the CAC.

Moreover, Article 14 of the Measures provides that a data exporter should apply for a new assessment 60 working days prior to the expiration of the existing CBDT security assessment result if the CBDT needs to be continued.

Legal Ramifications for Breach of the CBDT Security Assessment Requirement

According to the Measures, if the CAC discovers that a data exporter has been conducting CBDT activities that do not conform to the security assessment requirement (including the security assessment result), the data exporter will be notified to terminate the CBDT. To resume conducting CBDT activities, the data exporter will need to rectify its non-compliance and to re-apply for the CBDT security assessment with the CAC.

Aside from the enforcement stipulated under the Measures, a data exporter conducting a CBDT in violation of the Measures may also be subject to the penalties under the CSL, the DSL and the PIPL.

Suggested Actions and Measures for MNCs ahead of the Implementation of the CBDT Security Assessment

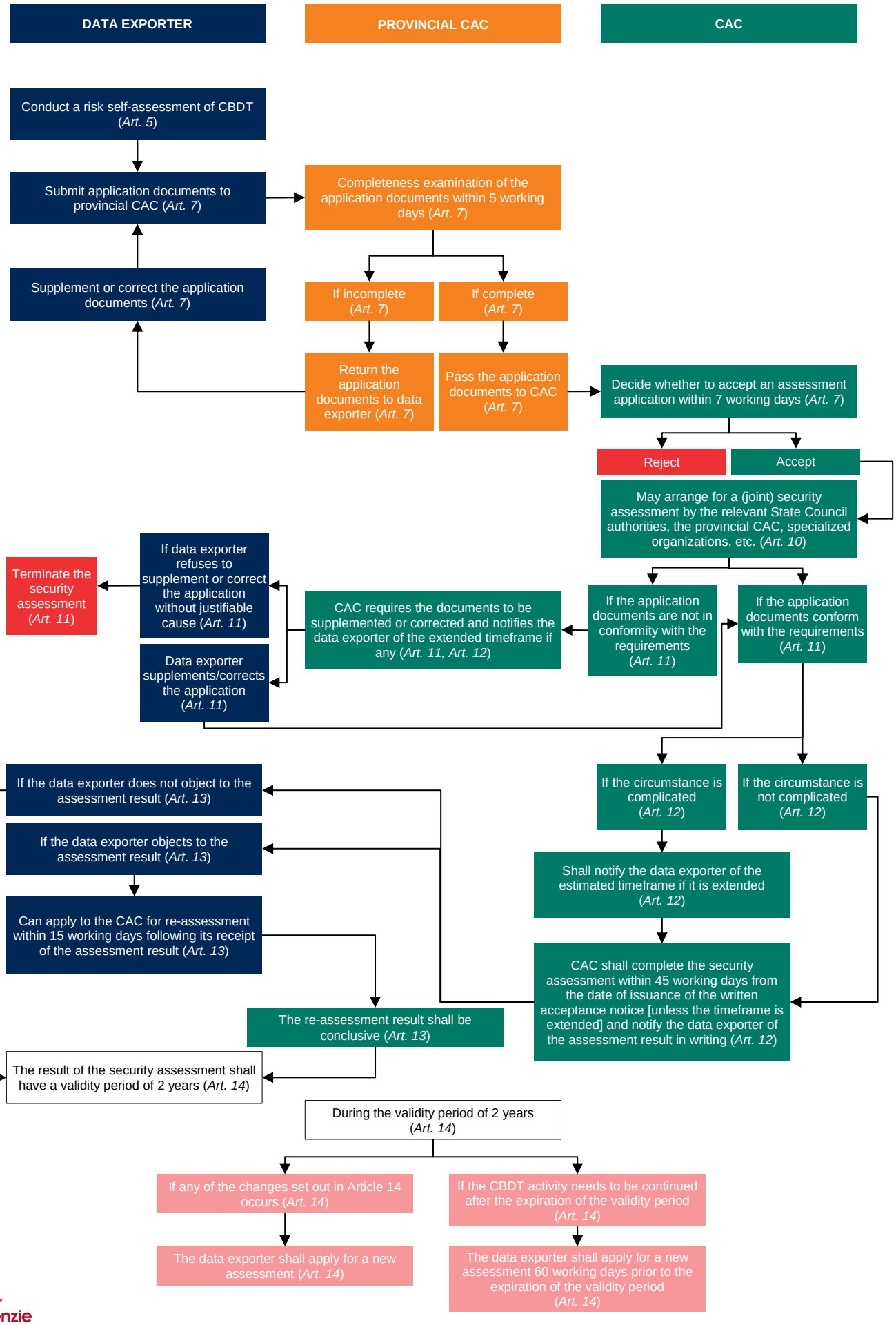
While the Measures will be implemented from 1 September 2022, a grace period is stipulated under the Measures whereby CBDT activities carried out prior to the implementation of the Measures that are not in compliance with the provisions of the Measures (i.e., the CBDT activities that have not been cleared by the CAC through the security assessment process) should be rectified within six months from the effective date (i.e., until 1 March 2023). While the grace period of six months is helpful, MNCs should act promptly to ensure compliance with the Measures before 1 March 2023 given the lengthy process (at least four months as analyzed above) and the coordinated effects to be involved.

Therefore, it is imperative for companies operating in China (if not doing so already) to act as quickly as possible to assess whether the security assessment requirement will be applicable. Companies should therefore:

- conduct data mapping and data inventory
- quantify the number of individuals whose personal information are processed and provided abroad,
- identify cross-border data flows including the relevant overseas recipients and corresponding global or regional IT systems / applications located outside China where data originating from China is received and processed; and
- determine if local systems or database solutions in China are available or need to be established and deployed.

Despite the lack of clarity around various technical and practical points concerning the CBDT security assessment, which are expected to be clarified or ironed out by the CAC before or concurrently with the initial implementation of the Measures, the action items listed above would (a) lay the solid ground for a data exporter to assess and determine if the use of the China SCCs or the application for the CBDT security assessment would be the applicable legal mechanisms for CBDT, and (b) form part of the work to be conducted in preparing the cross-border data transfer agreement based on the China SCCs (if the CBDT security assessment requirements are not triggered) or the security self-assessment and the Legal Document (where the CBDT security assessment requirements are applicable).

We expect a slew of applications to be filed with the CAC on or shortly after 1 September 2022. It remains to be seen if the CAC will handle these applications smoothly during the first month or two. There may be practical guides and tips that would be made available from the initial applications filed with the CAC. Therefore, we suggest that companies in China keep close track of the CAC's practice, watch out for further guides and procedural requirements and prepare / update the security self-assessment and application document preparation before initiating the CBDT security assessment application with the CAC.



Contact Us

Zhenyu Ruan
Senior Counsel, Shanghai
zhenyu.ruan@bakermckenziefenxun.com

Yangdi Zhao
Associate, Shanghai
yangdi.zhao@bakermckenziefenxun.com

Cora Wu
Associate, Shanghai
cora.wu@bakermckenziefenxun.com