ALLEN & OVERY | 朗悦
LANG YUE | 安理国际律师事务所

China promulgates measures on security assessment for cross border transfer of data

July 2022

On 7 July 2022, the Cyberspace Administration of China (**CAC**) released the Measures on Security Assessment for the Cross-border Transfer of Data (the **Measures**). As a step in the process of further detailing the mandatory governmental security assessment for transferring data outside Mainland China (**Security Assessment**), which has been laid out in principle under the PRC Cybersecurity Law, the PRC Data Security Law, and the PRC Personal Information Protection Law (the **PIPL**), the adoption of the Measures signals a new era for regulating the cross-border transfer of data under PRC law.

Most importantly, the Measures articulate the conditions under which the Security Assessment is triggered, the procedure for the Security Assessment, and the factors to be considered by the cyberspace and other administrative authorities in conducting the Security Assessment.

The Measures largely follow a consultation draft published by the CAC in October 2021 (the **2021 Draft**), with some key revisions refining the scope and procedure of the security assessment mechanism to be implemented. Further to our last alert on the 2021 Draft, we will highlight these key changes in this updated overview.

New Measures requiring careful consideration for data exports, suggesting that all companies operating in China should review them with their chosen advisors to understand how they might impact their specific operations. Generally speaking, and in the M&A context, a change in control arising out of a share sale could very well trigger a refreshment of the CAC assessment under these new Measures. Legal compliance of onshore target companies will be an area subject to enhanced due diligence and remedial actions. In the employment context, under the Measure, organisations and individuals are “encouraged” to report any compliance violations. This may provide an additional avenue for disgruntled employees to lodge complaints with their employers or to make or threaten to make regulatory reports for leverage in employment separation discussions. These Measures may also raise additional complexities when a China-based organisation is faced with an overseas litigation or investigation conducted by foreign regulators. The Measures signal that companies should also be mindful of an increased risk of investigations conducted by the CAC and other relevant PRC regulators, concerned with violations of the new data and personal information security protection regimes. Companies with a need to transfer their data across the border of Mainland China, particularly multinationals, need to pay close attention to the Measures and any further practical guidance or rules that may be released by the authorities from time to time.

A unified mechanism for Security Assessment

The Measures serve as a response to various PRC laws calling for the establishment of a governmental security assessment mechanism for the cross-border transfer of certain data.

– Back in 2017, the PRC Cybersecurity Law required a Security Assessment for the cross-border transfer of important data and personal information by critical information infrastructure operators (CIIOs).

– Further strengthening the regulation, the PRC Data Security Law promulgated in 2021 required a Security Assessment for the cross-border transfer of important data for all data processors, not just CIIOs.

– Similarly, the PIPL also expanded the scope of data processors subject to Security Assessment, adding data processors that process personal information with an amount exceeding the thresholds set by the cyberspace authorities.

In short, under PRC law, the Security Assessment concerns two types of data: important data and personal information. There have previously been attempts to establish separate security assessment mechanisms for important data and personal information respectively, but eventually the authorities decided to adopt a unified approach, which led to the promulgation of the Measures.

As such, to understand the Measures and their impact on data processors' activities, it would be helpful to engage in a little discussion about the definitions of these two key terms under PRC law: important data and personal information.

Important Data and Personal Information

Important Data

While this concept of important data under PRC law was first mentioned in the PRC Cybersecurity Law in 2017, there has not been a unified definition across various legal documents. In the Measures, important data (Important Data) are defined as those data that "once tampered with, destroyed, leaked, or illegally acquired or used, may endanger national security, economic operations, social stability, public health and safety, etc."

This definition outlines the contours of Important Data but does not set up a practical guide which companies can follow to classify and categorise their data. The PRC authorities have released several rounds of consultation drafts for a national standard specifying how to identify Important Data (the Identification Guide of the Important Data (Draft for Comments)). Based on these drafts, Important Data are mostly concerned with the following matters:

– Economic operations

– Demography and health

– Natural resources and environment

– Science and technology

– Security protection (physical and cyber)

– User data and usage data for certain sensitive application services

– Activities of governmental authorities

Based on the latest draft of the guide released on 13 January 2022, specific categories and characteristics of Important Data relevant for particular districts and/or industries will be further elaborated on by the regulators overseeing that district and/or industry. Consequently, businesses should closely monitor any legislative development at the local and industry levels applicable to their localities and industries. When necessary, businesses should work with their external counsel to identify the need to consult various authorities when determining whether they are processing any Important Data.

Personal Information

Unlike Important Data, the definition of personal information under PRC law (Personal Information) is more straightforward. Article 4 of the PIPL provides that Personal Information refers to "a variety of information relating to an identified or identifiable natural person that is recorded electronically or otherwise, excluding anonymised information." Article 28 of the PIPL provides that sensitive personal information (Sensitive Personal Information) refers to "personal information that, once leaked or illegally used, may easily infringe on the dignity of natural persons or endanger personal or property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts tracking and other data, as well as the personal information of minors under the age of 14." The Measures should be read together with these definitions as the PIPL is one of the sources of the Measures.

Scenarios triggering Security Assessment

Article 4 of the Measures specifies that a Security Assessment must take place in any of the following scenarios:

– where a data processor is exporting Important Data;

– where a CIIO or a data processor that processes Personal Information of more than one million data subjects is exporting Personal Information;

– where a data processor exporting Personal Information has already, cumulatively, exported Personal Information of more than 100,000 data subjects or Sensitive Personal Information of more than 10,000 data subjects since 1 January of the previous year;

– other situations determined by the CAC.

Like the 2021 Draft, the Measures take a hybrid of qualitative and quantitative approaches to determining the scenarios triggering Security Assessment:

– For Important Data, all data processors, whether they are a CIIO or not, need to apply for a Security Assessment – even if they only transfer one piece of such data out of Mainland China.

– For Personal Information, the need for a Security Assessment is determined by (1) the nature of the data processor (CIIO or not) or (2) the volume of Personal Information that the data processor processes or cumulative exports.

It is worth noting that the Measures clarify the length of the period applicable to the accumulation volume test, thus eliminating the risk for small and medium data processors to become subject to Security Assessments only because their export of Personal Information has reached the threshold (say of more than 100,000 data subjects) during a much more extended period of time (say over ten years).

However, in the finalised measures, the CAC did not address another concern around which many multinationals were seeking guidance; namely, whether intra-group data transfers would receive streamlined and less regulated treatment. The CAC has not created an express exemption in the Measures. It remains to be seen whether any further guidelines or exemption will be adopted in this regard after the Measures have been put into practice.

Self-assessment

According to Article 5 of the Measures, data processors shall carry out self-assessment before applying for a Security Assessment (**Self-assessment**), and in Article 6, a self-assessment report, as a work product of the Self-assessment, is identified as one of the application documents that should be submitted to the CAC when the data processor needs to file for a Security Assessment.

This Self-assessment is a side procedure that accompanies a Security Assessment and is not intended to apply to all situations where there is a cross-border transfer of data out of Mainland China. It should not be confused with the impact assessment requirement under Article 55 of the PIPL, which is to be conducted by data processors when exporting Personal Information regardless of whether one of the above triggering conditions for a Security Assessment has been satisfied.

In their Self-assessment, data processors are required to focus on the following items:

– The legality, legitimacy, and necessity of the purpose, scope, and method of the data transfer and the overseas recipient's data processing activities;

– The scale, scope, category, and sensitivity of the data to be transferred as well as the risks that the data transfer may bring to national security, public interests, and the legitimate rights and interests of individuals or organisations;

– The responsibilities and obligations that the overseas recipient undertakes, and whether the overseas recipient's management and technical measures and capabilities for fulfilling the responsibilities and obligations can ensure the security of the data to be transferred;

– The risk of data being tampered with, destroyed, leaked, lost, transferred, or illegally acquired or used during or after the data transfer, and whether there are unobstructed channels for safeguarding personal information rights and interests, etc.;

– Whether the data transfer agreement or other legally binding documents (collectively, Data Transfer Legal Instruments) to be concluded with the overseas recipient fully stipulate the responsibilities and obligations in relation to data security protection;

– Other matters that may affect the security of the data transfer.

As we will further illustrate below, the risk factors that the CAC focuses on in its Security Assessment have a substantial overlap with the above items that should be covered by data processors' Self-assessment. Data processors are therefore advised to retain external counsel early on at the Self-assessment stage to ensure that a robust self-assessment report is prepared and submitted.

The process for Security Assessment

Compared to the 2021 Draft, the Measures refine the steps of Security Assessment, add procedures for data processors to appeal a Security Assessment decision, and further adjust the time limits for the authorities to handle the assessment. For details, please refer to the flowchart annexed at the end of this document.

In the Security Assessment, the CAC is required to focus on the risks that the data transfer may bring to national security, public interests, and the legitimate rights and interests of individuals or organisations, mainly including the following items:

– The legality, legitimacy, and necessity of the purpose, scope, and method of the data transfer;

– The impact of the data security protection policies and regulations and network security environment of the country or region where the overseas recipient is located on the security of the data to be transferred; whether the data protection level of the overseas recipient meets the provisions of the PRC laws, administrative regulations and the requirements of mandatory national standards;

– The scale, scope, category, and sensitivity of data to be transferred, and the risk of data being tampered with, destroyed, leaked, lost, transferred, or illegally acquired or used during or after the data transfer;

– Whether data security and data subject rights and interests can be fully and effectively guaranteed;

– Whether the Data Transfer Legal Instruments to be concluded between the data processor and the overseas recipient fully stipulate the responsibilities and obligations in relation to data security protection;

– Compliance with PRC laws, administrative regulations and departmental rules;

– Other matters that the CAC finds it necessary to assess.

A Security Assessment will generally be valid for two years unless certain changes take place and trigger a re assessment (Article 14 of the Measures). Among those triggers, some may need clarification. For example, what constitutes a "change in the actual control" of the overseas data recipient "that may affect the security of the exported data"? It is clear that certain notification processes must be built into the agreement with the overseas data recipient to ensure that the data exporter is aware of such a change in a timely manner, in particular when publicly available information is limited. This leads to our next topic: the Data Transfer Legal Instrument to be concluded between the data exporter and the overseas data recipient in respect of the cross border data transfer.

Data Transfer Legal Instruments

Whether there is a Data Transfer Legal Instrument in place between the data exporter and the overseas data recipient to address the parties' responsibilities and obligations is one of the focuses of both the Self-assessment and the Security Assessment conducted by CAC. Compared to the 2021 Draft, for Security Assessment, the Measures allow more categories of legal instruments in addition to typical data transfer agreements, such as a unilateral commitment letter or undertaking letter by the overseas recipient.

Article 9 of the Measures sheds some light on the elements that a qualified Data Transfer Legal Instrument should address:

– the purpose, method and scope of the data transfer, the purpose and method etc. of data processing by the overseas data recipient;

– the location and duration of data storage overseas, and the processing measures after the expiry of the data storage period, the fulfilment of the agreed purpose of the data processing or the termination of the Data Transfer Legal Instrument;

– restrictive requirements on the further transfer of data by the overseas data recipient to other organisations and individuals;

– security measures that the overseas data recipient should take if there is a substantial change of control of the overseas recipient or a substantial change in its business scope, or in the data security protection policies and regulations, as well as the network security environment of the country or region where the overseas recipient is located, or other force majeure events, which make it difficult to ensure data security;

– remedies, responsibilities and dispute resolution methods for any breach of data security protection obligations as provided by the Data Transfer Legal Instrument; and

– requirements for proper emergency responses and approaches for individuals to safeguard their data subject rights where there is a risk of data being tampered with, destroyed, leaked, lost, transferred, or illegally acquired or used etc.

The above requirements largely resemble what was envisioned by the CAC for a Chinese version of the standard contractual clauses for the cross-border transfer of data, as reflected in the draft Provisions on the Standard Contract for Personal Information Cross-border Transfer released on 30 June 2022, although the standard contract clauses are designed for scenarios where a mandatory Security Assessment is not triggered.

Ratification period

The Measures will come into force on 1 September 2022. In addition, compared to the 2021 Draft, the Measures provide for a six-month rectification period for "any noncompliant cross-border data transfer activities that have already been launched before the implementation of the Measures". It is not entirely clear as to whether this rectification obligation also applies to cross-border data transfer activities that were launched but completed before 1 September 2022. A reasonable interpretation would suggest that it does not, but data processors should closely monitor whether the authorities take a different view.

Suggested action items

In light of the tight timeframe between now and 1 September 2022, when the Measures will take effect, we recommend that:

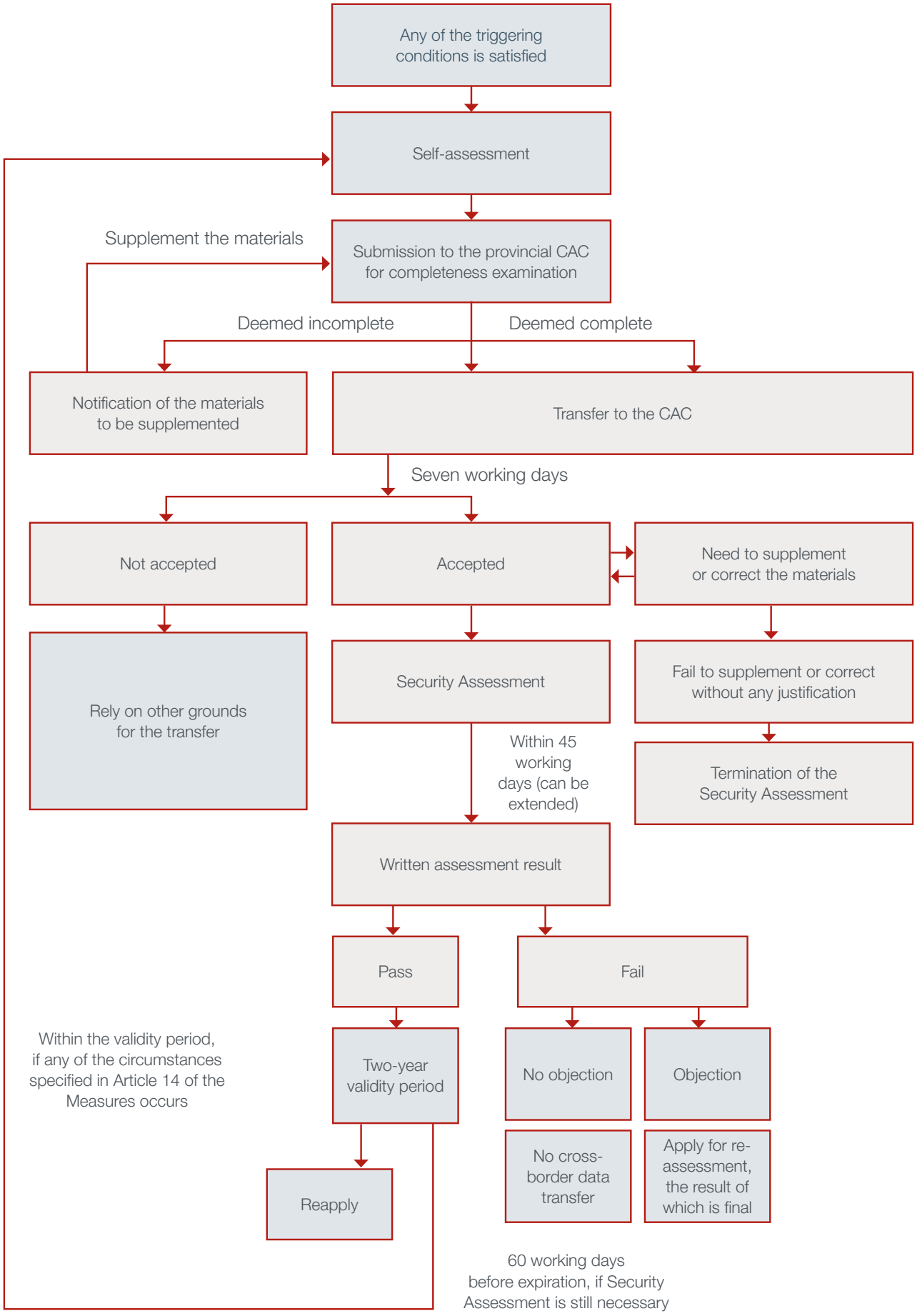
– Businesses should immediately conduct a complete mapping of all their data activities that lead to exporting data out of Mainland China and evaluate whether such activities may have triggered or, with the lapse of time, will trigger the need for a Security Assessment. We recommend that every business conduct a self-assessment. Businesses should act fast and well ahead of the deadline of 1 September 2022.

– Based on the evaluation, businesses should consider (i) whether to localise their data practice and/or (ii) filing an application for a Security Assessment if the triggering conditions have been satisfied and the cross-border data transfer is a must for their operations.

– Businesses should assume that a Security Assessment will be required and mobilise both internal and external resources to form a task force to address this issue. It is a dynamic, long-term process as the mechanism is just about to be put into practice and various practical issues will arise. The CAC and related authorities are likely to release further guidance in this regard. Businesses should pay close attention to such guidance and, when necessary, actively seek clarifications from the CAC and other related authorities.

– Finally, parties looking to enter into transactions or arrangements involving data flowing in and out of China should give sufficient consideration to potential regulatory compliance implications. With cross-border data transfer becoming regulated in a more structured manner, it would be advisable to assess early and build in compliance obligations as well as appropriate standard contract clauses in the applicable transaction documents.

The process for Security Assessment flowchart



Key contacts

Eugene Chen
Registered Foreign Lawyer – A&O – Hong Kong
Tel +852 2974 7248
eugene.chen@allenovery.com

Jill Ge
Partner – A&O – Shanghai
Tel +86 21 2036 7124
jill.ge@allenovery.com

Victor Ho
Registered Foreign Lawyer, Cal – A&O – Hong Kong
Tel +852 2974 7288
victor.ho@allenovery.com

Jane Jiang
Partner – A&O – Shanghai
Tel +86 21 2036 7018
jane.jiang@allenovery.com

Melody Wang
Partner – Lang Yue
Tel +86 10 8524 6288
melody.wang@allenoveryly.com

Ran Chen
Counsel – Lang Yue
Tel +86 10 8524 6100
ran.chen@allenoveryly.com

Paul Jing
Counsel – Lang Yue
Tel +86 21 2067 685
paul.jing@allenoveryly.com

Susana Ng
Of Counsel – A&O – Hong Kong
Tel +852 2974 7015
susana.ng@allenovery.com

Richard Wagner
Registered Foreign Lawyer, WI – A&O – Hong Kong
Tel +852 2974 6907
richard.wagner@allenovery.com

Tiantian Wang
Counsel – Lang Yue
Tel +86 21 2067 6835
tiantian.wang@allenoveryly.com

CN
CA2207046