DEACONS
的近律師行

PRC Data Protection Updates

China Intellectual Property

12 August 2022

Complying with China's cross-border data transfer rules

Dora Si and Andy Yu

Complex data security regime

At a time when the digital economy is booming, and cross-border data activities are growing, China's complex data protection and cybersecurity rules can be a challenge for businesses. The export of personal data from China needs to be considered in the context of China's 3 underlying data protection laws: The Cybersecurity Law, The Data Security Law and the Personal Information Protection Law (PIPL).

According to Article 38 of the PIPL, a business wishing to carry out cross-border transfers of the personal information of China-based subjects, due to business needs, should satisfy *at least one* of the following conditions:

(1) passing an official security assessment conducted by the Cyberspace Administration of China (CAC);
(2) obtaining a personal information protection certification from a recognised organization;
(3) executing a contract, in a form prescribed by the CAC, with the data recipient; or
(4) other conditions provided in relevant laws and regulations, or by the CAC.

Major updates

The details for implementation of these conditions have been unclear until the recent release of a number of major updates by the Chinese Regulators that have shed light on the requirements of Article 38. In particular, the release of the long-awaited final version of the Measures for Security Assessment of Cross-border Data Transfer (the Measures) has elicited much discussion. However, businesses should take note of all the latest developments summarised below:

No.	Name of document	Status	Criteria / eligibility
(1)	"Measures for security assessment of cross-border data transfer" (数据出境安全评估办法)	Effective from 1 September 2022, ***but with retrospective effect***: personal information processors should rectify their cross-border transfer practice ***within 6 months*** after implementation.	A personal information processor who satisfies <u>one of the following criteria</u> is required to pass an official security assessment conducted by the CAC ("official assessment"): • ***important data*** is transferred outside Mainland China; • the personal information processor is a ***critical information infrastructure operator***; • the personal information of ***more than 1 million*** people is being processed; or • cumulatively, the personal information of more than 100,000 people, or the ***sensitive personal information*** of more than 10,000 people, has been transferred outside Mainland China since 1 January of the previous year.
(2)	"Guideline on security certification for cross-border transfer of personal information activities" (Guideline) (个人信息跨境处理活动安全认证规范)	Effective from 24 June 2022	This avenue of obtaining certification is available to intra-group company transfers of personal information, and personal information processors who are outside Mainland China, but are subject to the extra-territorial application of the PIPL. Further clarification on a number of issues is required, for instance, whether intra-group companies that meet one of the above prescribed criteria set out in the Measures, can be exempted from official assessment if they have already obtained a certification pursuant to this Guideline.

(3)	Consultation draft "Regulations for standard contract for cross-border transfer of personal information" (个人信息出境标准合同规定) and "Standard contract template" (个人信息出境标准合同)	Under consultation	A personal information processor who satisfies all of the following criteria may rely on a standard contract in the prescribed form to facilitate the transfer: (i) it is not a ***critical information infrastructure operator***; (ii) it does not process personal information of ***more than 1 million people***; and (iii) it has not, cumulatively, transferred the personal information of more than 100,000 people, or ***sensitive personal information*** of more than 10,000 people, outside Mainland China since 1 January of the previous year.

Practical steps for businesses

Although certain aspects of these latest developments may resemble the regulatory landscape concerning cross-border data transfer in other jurisdictions, such as the GDPR, there are key differences. Businesses that are GDPR compliant should still check that they comply with the PIPL. Therefore, it is important for businesses to review their practices as soon as possible. This is particularly given the retrospective effect of the Measures for Security Assessment of Cross-border Data Transfer and the relatively short time frame for rectification of 6 months.

(1) Businesses with operations in Mainland China, or targeting customers in Mainland China, should evaluate whether they can satisfy any of the conditions set out in Article 38 of the PIPL considering the categories and volume of data that they have processed and will process. However, it is important to bear in mind the duration of validity even if such conditions are met, e.g. the official assessment result is only valid for 2 years and it is currently unclear whether a certification, as set out in condition 2, will be permanent.

(2) Businesses should be aware that a self-assessment on the cross-border data transfer risk ("risk self-assessment") will be required in order to satisfy the official assessment condition set out in condition (1) of Article 38 above, and a personal information impact assessment report ("PIA report") is required to be submitted in order to meet conditions (2) and (3). Both the risk self- assessment and PIA report cover various fundamental issues which need to be considered including:

- Whether the processing activities (including the cross-border transfer element) satisfy the **requirements of necessity, legitimacy and lawfulness**? For instance, has separate consent been obtained from the data subjects, especially for cross-border transfer? Have the data subjects been informed of the details of the cross-border transfer, such as the name and contact of the data recipient, types and purposes of personal information being transferred, and the manner of processing?
- Are the more stringent requirements for processing **sensitive personal information** complied with? For instance, has separate consent been obtained for processing **sensitive personal information**? Also, before processing the personal information of children aged under 14 (which is considered as sensitive personal information), has consent from their parents or guardians been obtained, and has a separate set of rules for processing personal information of children been put in place?
- Is there any mechanism for the data subjects to exercise their rights?
- Are the contractual obligations imposed on the data recipients sufficient for data protection purposes?
- What is the level of data protection provided in the laws of the jurisdictions in which the data recipients are located?
- What are the risks of data breach and the measures adopted to mitigate such risks in the cross-border transfer?

(3) The practices addressing the issues raised above should be reflected in privacy policies and instruments for obtaining data subjects' consent, as well as in relevant internal protocols.

(4) Businesses are also required to put in place relevant data processing and/or transfer agreements (even in the case of intra-group transfers), setting out the rights and obligations of the transferor and the recipient of the data, as well as the rights of the individual data subjects. When negotiating the data processing or transfer agreements with third parties, such as IT service providers offering cross-border cloud services, businesses should prioritise high-risk data protection compliance issues that must be addressed. For instance, will any sub-processor receive personal information from the data recipient after it has been transferred out of Mainland China? Where is any sub-processor (and the data-hosting server) based, and is there any back-to-back agreement between the IT service provider and its sub-processor? Businesses should ensure that suitable warranties and indemnities are in place with relevant third parties to manage the legal risks arising from the tightening of the regulatory regime.

Whether a data exporter or data recipient, businesses should review their personal information protection practices, as well as their contractual obligations under any standard contract. As the regulations for cross-border data transfer continue to evolve, businesses will need to be proactive to remain compliant with the latest requirements.

Want to know more?

Annie Tsoi
Partner
annie.tsoi@deacons.com
+852 2825 9255

Catherine Zheng
Partner
catherine.zheng@deacons.com
+852 2825 9617

Dora Si
Partner
dora.si@deacons.com
+852 2826 5394

Ian Liu
Partner
ian.liu@deacons.com
+852 2826 5360