

Release of the Draft Measures on Security Assessment of Cross-border Data Transfer

November 2021

Introduction

On October 29, 2021, the Cyberspace Administration of China (“**CAC**”) released the much-awaited “Draft Measures on Security Assessment of Cross-border Data Transfer” (“**Draft Measures**”) for public comments through November 28, 2021. The Draft Measures are intended to provide guidance and clarifications for implementing the legal requirements for cross-border data transfer as laid down in the Cybersecurity Law (“**CSL**”), the Data Security Law (“**DSL**”) and the Personal Information Protection Law (“**PIPL**”).

This article summarises the key points of the Draft Measures as well as providing takeaways and compliance suggestions.

I. When is a security assessment required?

The Draft Measures provide that a security assessment is required under the following circumstances:

- (i) For critical information infrastructure operators (“**CII operators**”), all personal information and important data collected within China will be subject to a security assessment before cross-border transfer;
- (ii) For non-CII operators, important data collected within China will be subject to a security assessment before cross-border transfer. No clear definition of “important data” is currently available;
- (iii) As for personal information collected by non-CII operators, the Draft Measures have clarified the standard under the PIPL. Under the Draft Measures, cross-border transfer of personal information will be subject to a security assessment in the following circumstances:
 - (a) It is performed by a data processor who processes personal information of one million or more individuals.

This means that if the personal information of one million individuals is being processed by a personal information processor, a security assessment will be required regardless of the volume of data to be transferred. In practice, the number of individuals whose personal information is processed by many Internet (especially to-C) companies or multinational enterprises would reach this threshold.

- (b) The cumulative cross-border transfer of personal information of more than 100,000 individuals or the cumulative cross-border transfer of sensitive personal information of more than 10,000 individuals.

It is important to note that the “one-million threshold” is also prescribed by the Draft Cybersecurity Review Measures which provide that, if an operator who processes the personal information of one million users goes public abroad, it shall file an application to the CAC for cybersecurity review.

We note that the threshold triggering security assessments on cross-border transfer of sensitive personal information has been lowered significantly, although it remains to be seen how the time period for calculating the “cumulative” transfers will be defined.

II. Security assessment process

Before transferring data abroad, a data processor should carry out a self-security assessment, analysing the data to be transferred, the data transferor and the foreign data recipient.

Following completion of the self-security assessment, the data processor needs to apply for a CAC-led security assessment by submitting the self-assessment report to the relevant provincial CAC authorities.

As the Draft Measures indicate that the security assessment process by the CAC authorities could take at least two months, companies should prepare for cross-border data transfers well in advance.

In addition, each self-security assessment is valid for only two years. A new self-security assessment should be submitted to the relevant CAC authorities upon any intermediate change of circumstances affecting the security of cross-border transfers or, if the cross-border transfer will continue after the expiry of the two-year period, within 60 business days prior to the expiry of such period.

The timing of the security assessment process will also need to be considered in the context of mergers, acquisitions and share transfers. The affect of any change of control resulting from such a transaction on data assets will require careful legal analysis, affecting pre-transaction legal due diligence, structuring and drafting stages of the deal, as well as the timing of the final closing and transition period. Therefore, a proper assessment of data assets will become an important element of merger and acquisition transactions going forward.

III. Cross-border data transfer contract

In accordance with the Draft Measures, each submission for a security assessment by a data processor should include an agreement or other legal document entered into by the data processor with the overseas recipient which sets out, among other things, the purpose, method and scope of the data transfer, the requirements for overseas storage of such data, the obligations and liabilities of the overseas recipient and the dispute resolution mechanism. The Draft Measures do not clarify whether such an agreement should be a separate standalone agreement or whether such provisions may be included in an existing contract between the parties. This may be clarified in future.

The Draft Measures also do not clarify whether such agreement on cross-border data transfer is different from the standard agreement issued by the CAC, as set out in the PIPL (the "Standard PIPL Agreement"). Based on publicly available information, the CAC is in the process of drafting the Standard PIPL Agreement but no timeline for completion is currently available. Therefore, it is difficult to anticipate at this stage whether the Standard PIPL Agreement will include the provisions required in the Draft Measures, and further clarification will be needed as to the relationship between those two sets of data cross-border transfer agreements.

IV. Compliance suggestions

The Draft Measures have given a strong signal to companies that Chinese regulators will tighten up regulations on cross-border transfers of data. It is expected that these Measures are likely to be adopted soon given that the PIPL already took effective on November 1, 2021. Considering the hefty penalties levied on violations of the DSL and the PIPL, all companies should pay close attention to the requirements under the Draft Measures and plan ahead accordingly.

The complexity of cross-border data transfer compliance for companies will increase and become more time-consuming as it relates not only to cross-border data transfer within a corporate group, but also to the compliance between companies and their foreign suppliers, customers, investors and other relevant third parties. Proper business arrangements should be considered and put in place in order to ensure compliance with the law.

We, as a specialised data legal team, have been deeply engaged in data law and cybersecurity compliance for many years and have an established reputation in the industry for assisting numerous multinational companies and Chinese companies in their data compliance governance. We will closely monitor all changes to the Draft Measures as well as all related legislative developments. Please contact us if you would like to gain a deeper understanding of the Draft Measures or discuss your specific compliance recommendations.

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

Rui Bai Law Firm



Barbara Li
Head of Corporate
Data and TMT Practice Lead
+86 10 8540 4686
barbara.xb.li@ruibailaw.com



Sarah Xiong
Senior Attorney

+86 10 8540 4608
sarah.q.xiong@ruibailaw.com



Vancci Wan
Manager
+86 10 8540 4616
vancci.y.wan@ruibailaw.com

Xin Bai Law Firm



Kris Fan
Counsel
+86 21 5368 4009
kris.fan@xinbailaw.com

Tiang & Partners



Chiang Ling Li
Partner
+852 2833 4938
chiang.ling.li@tiangandpartners.com

www.ruibailaw.com

www.xinbailaw.com

www.tiangandpartners.com

The information contained in this document is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of professional advice or service by Rui Bai Law Firm, Xin Bai Law Firm and Tiang & Partners. Rui Bai Law Firm, Xin Bai Law Firm and Tiang & Partners have no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual law firm contact or your other advisers.

The materials contained in this document were assembled in November 2021 and were based on the law enforceable and information available at that time.

© 2021 Rui Bai Law Firm. All rights reserved.

© 2021 Xin Bai Law Firm. All rights reserved.

© 2021 Tiang & Partners. All rights reserved.