中倫律師事務所
ZHONG LUN LAW FIRM

China's Data Cross-border Rules are about to Fall into Place -Comments on the *Measures for Security Assessment of Data Cross-border Transfer (Exposure Draft)*

Peng Cai
Yangyang Su
From Zhong Lun Law Firm

Key Words: China, Cybersecurity, Data Cross-border Transfer

Summary: On October 29, 2021, the Cyberspace Administration of China released a notice on the *Measures for Security Assessment of Data Cross-border Transfer (Exposure Draft)*. The draft, which is the latest regulatory response to the issue of data cross-border security assessment, sheds light on comprehensive and strict supervision over cross-border transfer of data and provides clearer regulatory compliance guidelines for businesses involved.

Introduction

On October 29, 2021, the Cyberspace Administration of China ("**CAC**") promulgated *the Measures for Security Assessment of Data Cross-border Transfer (Exposure Draft)* ("***Exposure Draft***") for public comment.

The Exposure Draft, which is the latest regulatory response to the issue of data cross-border security assessment, clarifies comprehensive and strict supervision more thoroughly and explicates regulatory compliance obligations of businesses involved in data cross-border transfer.

This article is mainly divided into two sections. This first section outlines the legislative history of data cross-border transfer assessment and the legislative context of the *Exposure Draft*. The second section reviews the key contents of the *Exposure Draft* and examines changes at the regulatory level with respect to data cross-border transfer and key points of businesses' compliance obligations.

I. History of data cross-border transfer assessment legislation

On April 11, 2017, the CAC promulgated the *Measures for Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)* .

On June 13, 2019, the CAC promulgated the *Measures for Security Assessment of Cross-border Transfer of Personal Information (Exposure Draft).*

On June 10, 2021, *The Data Security Law of the People's Republic of China* ("***Data Security Law"***) was adopted at the 29th session of the Standing Committee of the 13th National People's Congress of the People's Republic of China and came into force on September 1, 2021.

On August 20, 2021, *The Personal Information Protection Law of the People's Republic of China* ("**Personal Information Protection Law**") was adopted at the 30th session of the Standing Committee of the 13th National People's Congress of the People's Republic of China and just came

into force on November 1, 2021.

On October 29, 2021, the CAC promulgated the *Measures for Security Assessment of Data Cross-border Transfer (Exposure Draft)*.

As can be seen, cross-border transfer of data has always been a focus and challenge in data legislation and a key factor that the legislature took into account at the beginning of the enforcement of the *Cybersecurity Law*. Subsequently, the legislation went through a stage of dividing cross-border data into two categories, namely, personal information and important data, and set up separate rules for them. With the data legislation framework largely completed, the cross-border assessment rules fall into place to facilitate the overall law enforcement.

II. Analysis of the main points of the *Exposure Draft*

1. The "Troika" [1]makes up the upper-level laws

With the promulgation of the *Data Security Law* and the *Personal Information Protection Law* in 2021, the upper-level laws on which data cross-border transfer assessment is based have been finalized, remedying the predicament where a lower-level law was in force, but an upper-level law, the basis of the former, was up in the air. The *Exposure Draft* clarifies the legal system for data cross-border transfer security assessment, with the "Troika", say, *the Cybersecurity Law*, the *Data Security Law* and *the Personal Information Protection Law*, acting as the upper-level laws and the *Exposure Draft* and other refined legal documents forming the lower-level laws. The legal system serves as the regulatory basis to guide the related work of data cross-border transfer security assessment.

2. Data processor is regarded as the subject of assessment

When the *Cybersecurity Law* and the *National Security Law* functioned as the upper-level laws for data cross-border transfer assessment, they defined the subject of assessment as "network operator", which was not precisely defined but at least clearly interpreted. One reason behind may be that it could mitigate the contradiction between the upper-level laws and the lower-level laws.

With the clarification of the upper-level laws by the *Exposure Draft* which deals with security assessment of data cross-border transfer, it is more accurate to use "data processor" as defined in the *Data Security Law* instead of the previously employed “network operator” to refer to the subject of assessment. This is one of the highlights of the *Exposure Draft* that in a way avoids a series of ambiguities in the application of the law caused by the unclear definition of the subject of assessment.

3. Return to the unified supervision model

As can be seen from the legislative history, the issue of data cross-border transfer assessment has undergone a shift from a unified supervision model of "important data + personal information" to a separate supervision model of "personal information", and then back to the unified supervision

[1] "Troika" means the *Cybersecurity Law,* the *Data Security Law* and the *Personal Information Protection Law*, the three upper-level laws that shape the regulatory system of China's cybersecurity and data protection.

model in the *Exposure Draft.*

The return to the "important data + personal information" model also signals that the regulator will no longer legislate separately on assessment of cross-border transfer of personal information and that of important data, thus alleviating businesses' increased regulatory compliance obligations associated with separate legislation.

4. Assessment model: a two-tier assessment process

Article 3 of the *Exposure Draft* provides that it is imperative to conduct security assessment for data cross-border transfer under the principle of combining ex ante assessment with continuous inspection as well as risk self-assessment with security assessment, so as to prevent security risks in data cross-border transfer and ensure orderly and free transfer of data in accordance with the law.

In addition to focusing on the supervision of the whole process of data cross-border transfer, Article 3 also specifies a two-tier assessment process of "risk self-assessment + security assessment" as illustrated below:

Process	Subject	Triggering Threshold	Assessment Items
Risk self-assessment (mandatory procedure)	Data processor	Article 5 Prior to data cross-border transfer, a data processor shall conduct self-assessment of the risks of outbound data, with an emphasis on the assessment of the following matters:	(I) Legality, appropriateness and necessity of the data cross-border transfer and the purpose, scope and method of overseas recipient's processing of the data; (II) The volume, scope, type and sensitivity of the data to be transferred; risks that the data cross-border transfer may pose to national security, public interests and the legitimate rights and interests of individuals or organizations; (III) Whether the management, technical measures and capabilities of the data processor in the data transfer will suffice to prevent data leakage, damage and other risks; (IV) 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 will ensure the security of the data cross-border transfer; (V) Risks of leakage, damage, tampering and abuse of data after the data is transmitted abroad and further transferred, and whether the channels for individuals to maintain their rights and interests in personal information are unblocked; and (VI) Whether the relevant contract for the data cross-border transfer is concluded with the overseas recipient that fully specifies the responsibilities and obligations for data security protection.

+Security assessment (not a mandatory procedure)	Data processor applies to the regulator for security assessment	Article 4 To carry out data cross-border transfer, a data processor falling under any of the following circumstances shall, through the local cyberspace administration at the provincial level, apply to the Cyberspace Administration of China for security assessment of outbound data: (I) The outbound data is personal information and important data collected and generated by an operator of Critical Information Infrastructure; (II) The outbound data contains important data; (III) A personal information processor that has processed personal information of more than one million people provides personal information overseas; (IV) The personal information of more than 100,000 people or sensitive personal information of more than 10,000 people is transferred overseas accumulatively; or (V) Other circumstances under which security assessment of data cross-border transfer is required as prescribed by the CAC.	Article 8 Security assessment of outbound data shall focus on the assessment of risks that data cross-border transfer may pose to national security, public interests and the legitimate rights and interests of individuals or organizations, mainly including the following items: (I) Legality, legitimacy and necessity of the purpose, scope and method of the data cross-border transfer; (II) The impact of the data security protection policies and regulations and the network security environment of the country or region where the overseas recipient is located on the security of the outbound data; and whether the data protection level of the overseas recipient meets the requirements of the laws, administrative regulations and mandatory national standards of China; (III) The volume, scope, type and sensitivity of the outbound data, and whether the data risks being leaked, tampered, lost, damaged, transferred, illegally acquired or illegally used when or after leaving the country; (IV) Whether the data security and the rights and interests in personal information can be adequately and effectively protected; (V) Whether the contract between the data processor and the overseas recipient includes sufficient provisions on the responsibilities and obligations for data security protection; (VI) Compliance with China's laws, administrative regulations and departmental rules; and (VII) Other matters that the CAC considers necessary to be assessed.

Risk self-assessment: In this two-tier assessment process, the risk self-assessment is a mandatory

process that a data processor must go through before transferring data abroad. The self-assessment requirement, however, does not limit the volume, scope and purpose of the data transfer. For our understanding, it is triggered when a data processor conducts data cross-border transfer. Thus, a data processor needs to carry out risk self-assessment as long as it conducts any data cross-border transfer. This is the regulatory compliance obligation that a data processor must fulfill in data cross-border transfer.

Security assessment: The security assessment by the competent authority is not a mandatory process. Only when a data processor who meets a certain threshold and carries out data cross-border transfer will it need to apply to the regulator for security assessment. After the application is submitted, the regulator will conduct the assessment according to the assessment items set out in the *Exposure Draft.* The adjustments to assessment items and assessment process are explained relatively clearly in the *Exposure Draft*. Among all those adjustments, the change to the conditions for security assessment constitutes a big breakthrough, which will be discussed in the next part.

5. Core: significant adjustments to statutory obligations of applying for security assessment

Article 4 of the *Exposure Draft* makes significant adjustments to the conditions under which data processors have a statutory obligation to apply for security assessment. It also greatly expands the scope of data processors with such obligation. The chart below compares and briefly comments on the conditions that trigger that obligation under the *Exposure Draft* with those under its 2017 version - the *Measures for Security Assessment of Personal Information and Important Data to be Transmitted Abroad* ("***2017 Version***").

Article 4 of *the Exposure Draft*	Article 9 of *the 2017 Version*	Briefly Comparative Analysis
(I) The outbound data is personal information and important data collected and generated by an operator of Critical Information Infrastructure;	(iv) The data to be transmitted abroad contains network security information about system vulnerabilities or security protection, among others, of Critical Information Infrastructure; (v) A Critical Information Infrastructure operator provides personal information and important data abroad;	*The Exposure Draft* expands the data scope of the Critical Information Infrastructure that may provoke an application for security assessment.
(II) The outbound data contains important data;	(iii) The data to be transmitted abroad contains data in the area of nuclear facilities, chemical biology, defense industry, population or health, or data of large-scale project activities or marine environment or sensitive geographic information;	The "important data" needs to be further detailed by the regulator, and data processors should pay attention to the fact that once the data processed is likely to be identified as important data, they are statutorily obligated to apply for security assessment.

(II) The outbound data contains important data;	(iii) The data to be transmitted abroad contains data in the area of nuclear facilities, chemical biology, defense industry, population or health, or data of large-scale project activities or marine environment or sensitive geographic information;	The "important data" needs to be further detailed by the regulator, and data processors should pay attention to the fact that once the data processed is likely to be identified as important data, they are statutorily obligated to apply for security assessment.
(III) A personal information processor that has processed personal information of more than one million people provides personal information overseas;		The *Exposure Draft* introduces a "subject+ act" criterion. The "subject" is defined as a personal information processor that has processed personal information of one million people and the "act" is defined as providing personal information overseas. As we understand it, this criterion is quite broad. It can be interpreted in a way that any subject who processes personal information of more than one million people may be obliged to apply for security assessment as long as it provides personal information overseas, regardless of the volume of information provided. In practice, personal information processors can easily meet the "subject" requirement. Since it is highly likely for personal information processors to reach the "subject +act" criterion, they need to pay particular attention to their statutory obligations of applying for security assessment under this criterion.
(IV) The personal information of more than 100,000 people or sensitive personal information of more than 10,000 people is transferred overseas accumulatively; or	(i) The data to be transmitted abroad contains, or contains in aggregate, the personal information of more than 500,000 users; (ii) The volume of the data to be transmitted abroad is more than 1,000 gigabytes;	The *Exposure Draft* adopts the concept of accumulation. This means that, in the absence of any other limitation on the requirement for applying for security assessment, whenever personal information or sensitive personal information is transferred overseas in the statutory accumulative volume, the data processor is obliged to apply for security assessment.
(V) Other circumstances under which security assessment of data cross-border transfer is required as prescribed by the CAC.	(vi) Other data which may affect national security or social and public interests, and is necessary for assessment as determined by the industrial authority or regulator. If there is no definite industrial authority or regulator, the CAC shall organize the assessment.	This is a catch-all provision with room for further interpretation in *the Exposure Draft*.

6. Other changes

In addition to the above important adjustments, the *Exposure Draft* further makes the following new changes:

1) The assessment period is relatively fixed. The *Exposure Draft* sets a maximum assessment period of sixty-seven working days.

2) The focus of assessment is clear: Assessment will be around the legitimacy and necessity of data cross-border transfer, potential security risks and protection level of the overseas recipient and the country where it is located, the sensitivity of data to be transferred abroad and the adequacy of protection of individuals' rights and interests.

3) The requisite terms of cross-border contracts are definite: The *Exposure Draft* sets out necessary provisions on security liability involved in cross-border transfers of data, which will form an important part of the template for cross-border contracts to be formulated by the cyberspace administration under the *Personal Information Protection Law*.

4) The competent authorities conducting the assessment are certain: The assessment will be led by the national cyberspace administration and undertaken by the competent authority of the industry concerned, relevant departments of the State Council, the cyberspace administration at the provincial level, specialized agencies, etc.

5) The conditions for reassessment are adjusted: Compared with the two previous versions, the *Exposure Draft* sets more flexible factors for reassessment based on data security considerations. These factors include, among others, changes in the legal environment of the recipient and contractual changes that may affect the security of data cross-border transfer.

6) The setting of legal liability is still based on legal provisions: Except for revocation and rectification, the *Exposure Draft* does not create any new legal liability for violating the assessment rules. Processors who violate the *Exposure Draft* will be held administratively and criminally liable under the *Personal Information Protection Law* and the *Data Security Law.*

Conclusion:

With the successive enforcement of the *Data Security Law* and the *Personal Information Protection Law*, the relevant implementation regulations will also be pouring in. As a data cross-border assessment rule in the industry, the *Exposure Draft* is highly likely to be the first implementation rule that will be enforced after the *Personal Information Protection Law* comes into effect. The promulgation of the *Exposure Draft* reflects that the overall objective of data supervision is to encourage free transfer of data on the basis of data security. However, it also creates considerable regulatory compliance pressure on the vast majority of data processors. For data cross-border transfer, the most important thing for businesses to do is to improve their internal control so that their external regulatory pressure will be reduced. (This was explicitly suggested in our 2017 article *New Regulatory Compliance Challenges for Companies under Measures for Security Assessment of Personal Information and Important Data Cross-border Transfer).*

In this regard, businesses are advised to build an overall data regulatory compliance system. For those involved or likely to be involved in data cross-border transfer, construction and implementation of a self-assessment system for data cross-border transfer should be an important part of the regulatory compliance system in order to cope with the coming era of strict regulation.

Intern Yujie Chen and Huiting Wang also contribute to this article.