July 21, 2022

China Promulgates New Implementing Rules to Facilitate Cross-Border Transfers of Data

Background

Attorneys
Katherine Wang
David Chen

On July 7, 2022, the Cyberspace Affairs Commission ("**CAC**") of China issued the Measures on Security Assessment of Cross-Border Data Transfer (the "**Security Assessment Measures**"), which sets out the security assessment framework for cross-border data transfers. The Security Assessment Measures will become effective on September 1, 2022. In conjunction with the issuance of the Security Assessment Measures, CAC also issued an interpretation guideline on the same day (the "**Interpretation Guideline**").

The Security Assessment Measures lay out the ground rules for a security assessment filing for cross-border data transfers that was stipulated in the Cybersecurity Law ("**CSL**") and the Personal Information Protection Law ("**PIPL**").

1. Security Assessment Is Required for Certain Cross-Border Data Transfers

Important Data

Under the CSL, when it is necessary for a critical information infrastructure operator ("**CIIO**") to transfer important data outside of China, a security assessment is required. The Data Security Law together with the Security Assessment Measures expands the security assessment requirement for cross-border data transfers of important data to all data processors ("**Data Processors**").

Personal Information

Under the PIPL, in order to transfer personal information ("**PI**") outside China, PI processors ("**PI Processors**") must meet at least one of the following conditions: (i) pass a security assessment, (ii) obtain a PI protection certification ("**PIPC**") from certain qualified institutions, (iii) enter into a contract with the data recipient in accordance with a standard contract prescribed by the CAC, or (iv) fulfill conditions stipulated in other laws or regulations. Additionally, the PIPL requires that CIIOs and PI Processors that process a certain amount of PI exceeding CAC's prescribed threshold must undergo a security assessment prior to effecting any cross-border data transfer. The threshold is now prescribed in the Security Assessment Measures, as further discussed below.

When a Security Assessment Is Required

A security assessment will be triggered if the cross-border data transfer falls into any of the following scenarios:

i. transfer of "important data" by Data Processors (*"Important data" is defined as "any data that, once tampered with, sabotaged, leaked or illegally obtained or used, may endanger national security, economic operation, social stability, and public health and safety*);

ii. transfer of PI by CIIOs and Data Processors that process PI of more than one million individuals;

iii. transfer of PI by Data Processors that have transferred either PI of over 100,000 individuals or "sensitive" PI of over 10,000 individuals abroad since January 1 of the preceding year; and

iv. other situations as determined by CAC.

According to the Interpretation Guideline, cross-border data transfer includes (i) an outbound transfer of data collected and generated during a company's operation in mainland China and (ii) a remote access or use of data stored within mainland China by overseas institutions, organizations and individuals.

Self-Risk Assessment Required in Advance

Prior to applying for a security assessment with CAC, Data Processors shall first carry out a self-risk assessment, which involves evaluation of a number of factors that CAC will consider in a security assessment. The findings of the self-risk assessment shall be presented to CAC along with an application filing to CAC for a security assessment. Upon receipt of the security assessment filing, CAC will notify the Data Processor of its decision to either accept the filing if it determines that the filing falls within the scope of security assessment or reject the filing if it determines that the filing does not fall within the scope of security assessment. If accepted, CAC will have 45 working days to complete the assessment in coordination with other relevant regulatory authorities. CAC may extend the period of assessment due to the complexity of the filing or if additional supporting documents are required.

Review of Security Assessment Filing

During the course of a security assessment, CAC will primarily focus on the risks to national security, public interests and the legitimate rights and interests of individuals or organizations that the cross-border data transfer may cause. The factors that come into play include:

i. the legality, justification and necessity of the purpose, scope and method of the cross-border data transfer;

ii. the data security protection policies and regulations of the country or region where the overseas recipient is located, the impact of the network security environment on the security of the exported data, and whether the level of data protection of the overseas recipient meets PRC laws, administrative regulations, and national standards;

iii. the scale, scope, type, sensitivity of the exported data and the risk of the exported data being tampered with, destroyed, leaked, lost, onward transferred or illegally obtained or used during and after the cross-border data transfer;

iv. whether data security and PI rights are fully and effectively guaranteed;

v. whether the contract executed with the overseas recipient has fully addressed the responsibilities and obligations in terms of data protection; and

vi. compliance with PRC laws, administrative regulations and departmental rules, etc.

Cross-border data transfer of the relevant data will not be allowed if CAC does not approve the security assessment filing. Once CAC approves the security assessment filing, such approval will remain valid for two years and may be renewed within 60 working days prior to the expiration date. During the two-year period, the Data Processor is required to re-submit an application for security assessment if it encounters any circumstances that may affect the security of the exported data, such as changes in the purpose, method, scope, and type of the exported data and changes in the purpose and method of the processing of the exported data by overseas recipients.

Notwithstanding any approval of a security assessment filing, CAC has the power to order a Data Processor to terminate a cross-border data transfer, if CAC determines that such cross-border data transfer no longer meets data export security

management requirements. In such case, the Data Processor needs to re-submit an application for security assessment after taking necessary rectification measures.

Retroactive Effect

Notably, the Security Assessment Measures has retroactive effect for cross-border data transfers of relevant data conducted prior to its effective date. If a Data Processor fails to complete its security assessment for any of its cross-border data transfers of relevant data, it needs to rectify the failure within six months after the effective date of the Security Assessment Measures.

2. PIPC May Not Be a Feasible Route for Cross-Border Transfer yet

On June 24, 2022, the National Information Security Standardization Technical Committee issued the Guidance on Network Security Standardized Practice – Specification for Certification of Personal Information Cross-Border Processing (the "**Certification Specification**"). The Certification Specification has no legal effect and serves as an industry standard only. It provides that PI Processors may apply for PIPC from certain qualified institutions recognized by CAC, pursuant to which PI Processors may rely on PIPC to effect (i) intragroup cross-border transfers within a multinational company or an economic/business entity; and (ii) data processing activities conducted outside of China involving PI of individuals located in China subject to the extraterritorial jurisdiction of the PIPL.

Qualified institutions will primarily focus on whether the cross-border data transfer is legitimate, justifiable, and necessary and the security protection measures taken are legitimate, effective, and appropriate to the degree of risk when determining the grant of PIPC to PI Processors. In addition, qualified institutions will also take into account a number of factors in the application for PIPC, including:

i. whether the cross-border data transfer complies with laws and administrative regulations;

ii. the impact on the rights and interests of PI subjects, especially the impact of the legal environment and network security environment of foreign countries and regions; and

iii. other matters necessary to safeguard the rights and interests in relation to PI.

However, the list of qualified institutions has not been released to date, and therefore, as of the date of this article, it is not yet possible for companies to rely on PIPC to legitimize their cross-border data transfers.

3. Standard Contract May Be a Safe Harbor for Cross-Border Data Transfers of Personal Information

On June 30, 2022, CAC issued the draft Regulations on the Standard Contract for Cross-Border Transfer of Personal Information (the "**Draft Provisions**") for public consultation, which introduced a draft standard contract for the cross-border transfer of PI outside of China (the "**Draft PRC SC**"). As with the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Regulation ("**GDPR**") (EU) 2016/679 (the "**EU SCCs**") issued by the European Commission on June 4, 2021, the Draft PRC SC provides clarity on the terms and conditions to be agreed on between PI Processors as a data exporter and an overseas recipient as a data importer with respect to cross-border data transfers of PI to third countries. When finalized, the Draft PRC SC can be used to comply with requirements under the PIPL for cross-border data transfers of PI out of China that do not need to undergo a security assessment.

As the terminology used in the Draft PRC SC and the EU SCCs are markedly different, the table below highlights the differences in the terms used frequently in this article.

PIPL or Draft PRC SC	GDPR or EU SCCs
PI Processor	data controller (or data exporter)
overseas recipient	data importer (could either be a data controller or a data processor)
entrusted processor	data processor
PI Protection Impact Assessment ("**PIPIA**")	data protection impact assessment ("**DPIA**")

The Draft PRC SC and EU SCCs are structured differently, with the former designed to address different types of cross-border data transfer scenarios in one standard contract and the latter having different sets of standard contractual clauses catering to different cross-border data transfer scenarios: (i) controller to controller; (ii) controller to processor; (iii) processor to controller; and (iv) processor to processor. A comparison table of the Draft PRC SC and EU SCCs is set out below to illustrate the respective pertinent features.

	Draft PRC SC	***EU SCCs***
Scope of Application	PI Processor may enter into a contract to effect a cross-border data transfer (the "**Standard Contract**") only if the following conditions are satisfied: i. it is not a CIIO; ii. it processes PI of fewer than 1 million individuals; iii. it has provided PI of fewer than 100,000 individuals overseas in aggregate since January 1 of the preceding year; and iv. it has provided sensitive PI of fewer than 10,000 individuals overseas in aggregate since January 1 of the preceding year.	No similar prerequisites for adopting EU SCCs.
PIPIA/DPIA	Prior to any cross-border data transfer, PI Processors shall carry out a PIPIA and file such assessment findings with the relevant regulatory authorities. The assessment encompasses the following criteria: i. legality, legitimacy and necessity of the purpose, scope and method of processing; ii. quantity, scope, type and sensitivity of PI to be transferred overseas, and the possible risks to the rights and interests of the PI subjects; iii. whether the administrative and technical measures undertaken by, and capabilities of, the overseas recipient are able to guarantee the security of PI;	a. Data exporters shall carry out a transfer impact assessment, which shall assess whether the laws and practices of the destination country could prevent the data importer from complying with the EU SCCs. b. On the other hand, a DPIA is a more comprehensive assessment, which is mandatorily required where data processing is likely to result in a high risk to the rights and freedoms of natural persons.

	iv. risks of leakage, damage, tampering and abuse of PI after it is transferred overseas; v. whether the channels for PI subjects to safeguard their rights and interests in PI are unobstructed; vi. impact of PI protection policies and regulations of the country or region where the overseas recipient is located; and vii. other matters that may affect the security of cross-border data transfer of PI.	
Onward Transfer	a. Overseas recipients are prohibited from any onward transfers of PI to a third party unless the following conditions are met: i. there must be a genuine need to provide PI for business purposes; ii. PI subjects have been informed of the identity and contact information of the third party, the processing purposes and methods, types of PI involved, and the methods and procedures for exercising the rights of the PI subjects, and separate consent of the PI subjects is obtained, unless separate consent is not required by relevant PRC laws and regulations; iii. a separate written agreement needs to be executed between the overseas recipient and any third-party recipient to ensure that such third party protects PI at a level not lower than the standard of protection provided by relevant PRC laws and regulations b. Overseas recipients shall bear joint and several liability in respect of any damages caused to PI subjects by virtue of onward transfer of PI to third parties.	An entity that is not a party to the EU SCCs may, with the agreement of the parties, accede to such agreement at any time, either as a data exporter or data importer.
Regulatory Matters	a. Within ten business days of the effective date of the Standard Contract, it shall be filed with the provincial CAC, along with a report documenting the assessment results of the PIPIA in compliance with relevant laws and regulations and national standards.	a. No affirmative filing requirement on the part of data exported, unless required by regulatory authorities. b. No explicit requirement to enter into new EU SCCs if there is a change in

	b. A new Standard Contract shall be entered into if any material changes in the processing activities or laws and policies of the destination country since the execution of the Standard Contract occurs.	the circumstances relating to the data transfer.
Transparency and Disclosure	a. The identity and contact information of any overseas recipient must be disclosed to PI subjects via reasonable means. b. A copy of the Standard Contract must be provided to PI subjects upon request, which shall include disclosure regarding all basic information regarding the processing details of the cross-border data transfer contemplated by the parties, including but not limited to the purpose of transfer, method of transmission, retention period of transferred PI, etc. c. The Draft PRC SC, unlike the EU SCCs, require additional disclosure of the quantity of PI transferred.	a. In the case of a data importer acting in the capacity of a data controller, the identity and contact information of such data importer must be disclosed. b. Disclosures required to data subjects are similar to that required by the Draft PRC SC, except that the Draft PRC SC additionally requires disclosure of the quantity of data transferred. c. Unlike Draft PRC SC, data importers appear to have an affirmative duty to provide data subjects with a copy of the EU SCCs.
Data Transfer to Foreign Authorities	Generally prohibits providing PI to foreign judicial or law enforcement authorities, unless otherwise approved by relevant PRC regulatory authorities.	The data importer shall notify the data exporter and data subjects when it receives legally binding requests from public authorities.
Governing Law	PRC law.	Depends on the specific type of the EU SCCs. The governing law could be laws of the country within or outside the European Economic Area where the data importer is located.
Permitted Alterations	a. Parties may supplement the Standard Contract with additional clauses, which may be added by the parties in annex II of the Draft PRC SC. b. In the event of inconsistencies between the main body of the Draft PRC SC and the supplemented additional clauses, the main body of the Draft PRC SC will prevail.	a. The text of the EU SCCs may not be altered, except: i. to select which module of the EU SCCs to adopt depending on the role of the data exporter and importer and/or to make specific selections on issues left open in the EU SCCs (e.g., choice of governing law and dispute resolution forum); ii. to complete the text where necessary, e.g., to indicate the competent courts and

		regulatory authorities, and to specify certain time periods; iii. to complete annexes to the EU SCCs; and iv. to include additional safeguards to increase the level of protection of data. b. Parties may incorporate EU SCCs into a broader commercial contract, so long as the contractual provisions do not contradict with the incorporated EU SCCs, or otherwise prejudice the rights of data subjects.

4. Recommendations

The rules pertaining to cross-border data transfers have broad ramifications for companies with operations in China, especially for foreign companies that operate in China and have a genuine business need to transfer data to its group companies or business partners located outside of China, or to maintain its existing data-sharing arrangements.

While the Security Assessment Measures provide comprehensive guidance regarding security assessment filings, it creates operational hurdles for companies to facilitate cross-border data transfers, particularly when such transfers fall into any category that triggers a security assessment filing. Further, "important data" is broadly defined in the Security Assessment Measures, thereby adding a layer of uncertainty as to the specific circumstances under which a security assessment filing is required. The retrospective effect of the Security Assessment Measures is also anticipated to cause a profound impact across many different industries concerning cross-border data transfers.

As for intragroup cross-border transfers, a PIPC could potentially be another route for companies to effectuate cross-border data transfers. However, the rules pertaining to obtaining a PIPC are yet to be operationalized given that the CAC has not yet released a list of qualified institutions that can grant a PIPC.

CAC is in the process of soliciting comments from the public on the Draft Provisions until July 29, 2022. We will closely monitor the development of the Draft Provisions and updates to the Draft PRC SC. The Draft PRC SC, once finalized, may likely be the most viable method to facilitate cross-border data transfers where approval of security assessment filings are not required.