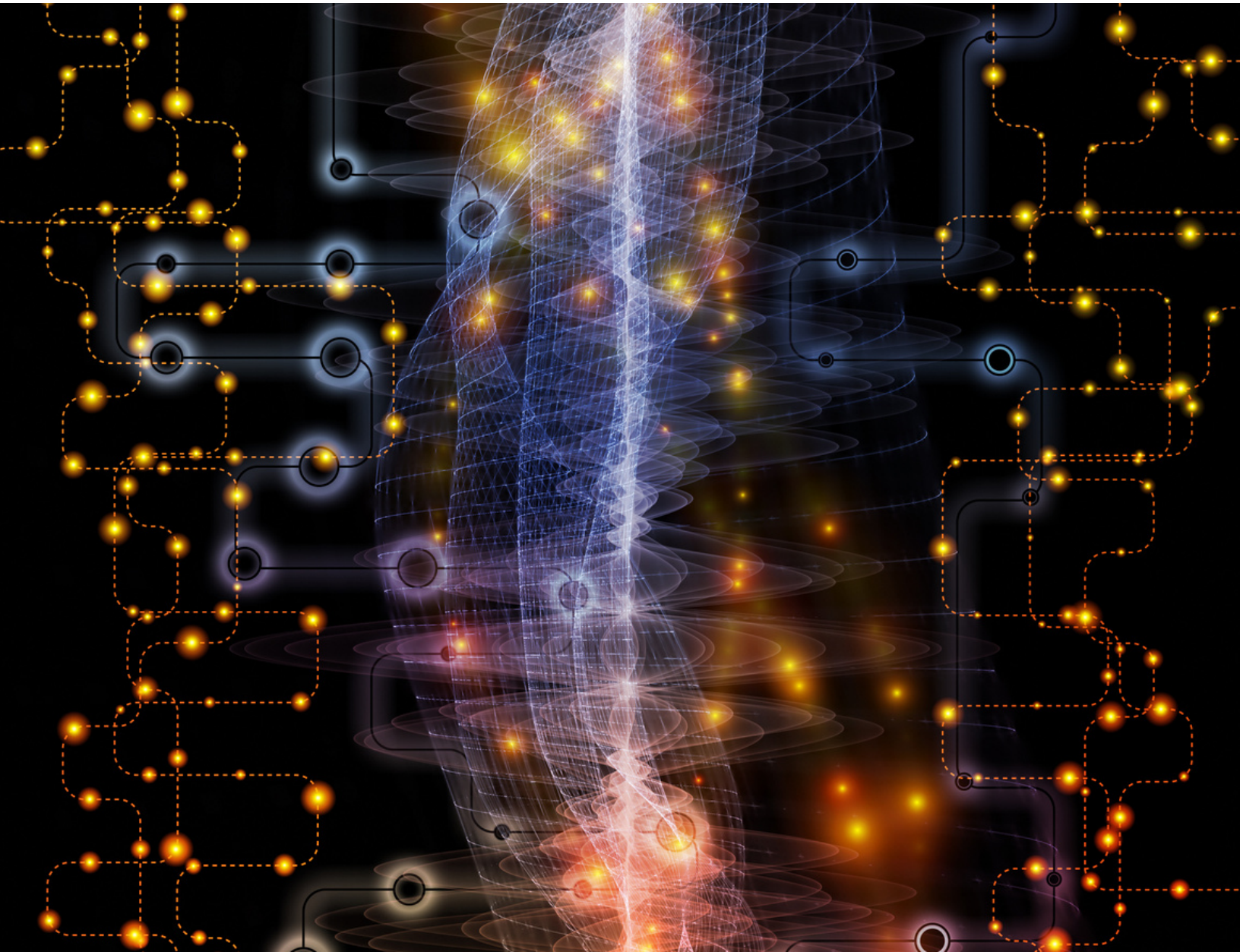
BRITISH CHAMBER OF COMMERCE IN CHINA
中国英国商会

POLICY BRIEFING:
CHINA RELEASES FURTHER REGULATIONS ON CROSS-BORDER DATA TRANSFERS



Executive Summary

China's cybersecurity and IT landscape is governed by three major laws and regulations being the:

- Cybersecurity Law ("CSL");
- Data Security Law ("DSL"); and
- Personal Information Protection Law ("PIPL").

Over the past month, the various regulatory bodies in China have circulated further measures and guidelines in regards to the cross-border transfer of data, handling of data, and the definition of "important data".

Navigating China's cybersecurity and IT regulations ranked as one of the top 3 cross-cutting challenges faced by British business over the past 12 months. These further guidelines and measures provide some welcome clarity in this area, but also place additional burdens on companies with regards to compliance and businesses need to be ready for when these come into force.

Overview of recent regulatory releases

RELEASE	DOCUMENT TYPE	RELEASE DATE	REGULATORY BODY
Practice Guidelines for Cyber Security Standards - Security Certification Specifications for Cross-Border Processing of Personal Information (the "Certification Guideline")	Practice Guideline (in force)	24 June 2022	National Information Security Standardisation Technical Committee
Measures on Security Assessment of Cross-border Data Transfer (the "Measures")	Regulatory measures (in force on 1 September 2022)	7 July 2022	Cyberspace Administration of China
Chinese Standard Contractual Clauses for Cross-border Personal Information Transfer	Consultation Paper	30 June 2022	Cyberspace Administration of China
Information Security Technology - Identification Rules of Important Data	Draft regulation	7 January 2022	National Information Security Standardisation Technical Committee

Practice Guidelines for Cyber Security Standards - Security Certification Specifications for Cross-Border Processing of Personal Information (the "Certification Guideline")

According to the PIPL, one of the three specified mechanisms by which cross-border transfers from China can be facilitated is by obtaining certification of cross-border data transfer from an organisation designated by the Chinese regulator. It is expected that such organisations will be designated for this purpose in the future. The Certification Guideline is a set of guidelines for handling such certification and for data handling in general.

Scope of Application

The Certification Guideline is expressly applicable in the following scenarios:

1. Cross-border personal information transfer between the subsidiaries or associate companies of multinational companies or other economic organisations.
2. Personal information processing activities outside of China of the personal information of natural persons in China, if the information is processed:
    a. For the purpose of providing products or services to natural persons located in China;
    b. To analyse or assess the conduct of individuals located in China; or
    c. Under any other circumstance as prescribed by the Chinese laws or regulations.

In circumstances set out at (1) above, where a company wishes to proceed with certification, the certification should be initiated by the entity in China, and that entity would bear the legal responsibility.

In circumstances set out at (2) above, if the data processor outside of China wishes to proceed with certification, the certification may be initiated by its designated

Basic Requirements for Certification

1. Legally Binding Agreement

There must be an agreement between the data controller and the recipient of the personal information outside of China (the "data recipient"). The agreement should include the details of the cross-border processing activities. Importantly, the data recipient must provide an undertaking to be bound by the relevant China laws and regulations and accept the supervision by the certification organisation.

2. Organisation Management

Both the data controller and the data recipient shall proceed as follows:

- Appoint a responsible person to conduct the data protection work, whose role is analogous to that of a data protection officer under the EU's General Data Protection Regulation (GDPR).
- Set up an organisation structure which handles data related works such as handling personal data access requests and complaints.

3. Personal Information Cross-Border Processing Rules

Both the data controller and the data recipient shall comply with the same set of personal information processing rules which cover basic matters such as the manner of handling personal data, the duration of data storage, and permissible locations for data relays, etc.

4. Impact Assessment

Before cross-border personal data transfer may proceed, an impact assessment needs to be conducted. It should evaluate items such as the legality of data transfer, whether the protection measures are compatible with the risk levels, whether the data subject's right will be undermined, etc.

5. Protection of Data Subject's Right

There are various requirements set out in regards to the protection of data subject's right, the key requirements are that data subjects have the:-

- Right of information, right to withdraw consent, and right to access;
- Right to require a copy of the relevant part of the agreement between the data controller and the data recipient;
- Right to reject automated decision making;
- Right to complain to Chinese regulators.

Measures on Security Assessment of Cross-border Data Transfer (the "Measures")

The transfer of data outside of China under certain circumstances requires prior Chinese government approval (referred to as a "security assessment") under the CSL, DSL and PIPL. The consent of the data subject is not sufficient. According to the PIPL, such security assessment is another one of the three specified mechanisms by which cross-border transfers from China can be facilitated.

The Measures were released on 7 July 2022, following the release of the relevant consultation paper last year, and will take effect on 1 September 2022. The Measures govern the security assessment process, and require that any transfer of data outside of China which fails to comply with the Measures is rectified by 1 March 2023. Any breach under the Measures may constitute a criminal offence and attract civil and administrative liabilities.

The Measures define "important data" and specify the circumstances when government approval for outbound transfer of data is needed.

What is "important data"?

The term "important data" is defined in the Measures as data that may endanger national security, economic operation, social stability, public health, and safety once they are tampered with, destroyed, leaked, or illegally obtained or used illegally.

This is similar to the definition in the draft regulation entitled Information Security Technology - Identification Rules of Important Data that we discuss in more detail below.

When is security assessment required?

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

1. A critical information infrastructure operator ("CII operator") transfers personal data outside of China;
2. A data controller (aka "data processor" in the Measures and other Chinese laws and regulations) who processes personal information of 1 million people or above transfers personal data outside of China;
3. A data controller (including one that is not a CII Operator) transfers "important data" outside of China;
4. A data controller who has since 1 January of the preceding year:
    a. Cumulatively provided personal information of 100,000 individuals outside of China; or
    b. Cumulatively provided sensitive personal information of 10,000 individuals outside of China transfers personal data outside of China;
5. Other situations as prescribed by the Cyberspace Administration of China ("CAC").

Sensitive personal information refers to the personal information that, once leaked or illegally used, can easily lead to the infringement of personal dignity of natural persons or the harm on personal and property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts and other information, as well as the personal information of minors under the age of 14.

The exemption from the requirement of obtaining Chinese government approval before proceeding with cross-border personal data transfers for companies which have not cumulatively transferred personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals outside of China every two years is welcome news to multinational companies.

Security Assessment Process

Before applying for a security assessment, a data controller should first carry out a self-assessment to evaluate issues including:

1. The data to be transferred and the necessity of the transfer;
2. The foreign data recipient;
3. The sufficiency of legal protection provided by the contract with the foreign data recipient; and
4. The risk of data leakage.

Following the completion of the self-assessment, the data controller may submit through the CAC at the provincial level for a security assessment by the CAC at the national level. The data controller must submit, among other things:

1. The report of the self-assessment;
2. The application form; and
3. The legal documents between the data controller and the foreign data recipient.

The Measures have provided for the following timeline for a security assessment:

1. Upon the receipt of application, the provincial CAC will assess whether the materials and information are sufficient within five (5) business days. The provincial CAC will pass the application to the national CAC if the application materials and information are deemed sufficient.
2. The national CAC will, by written notice, inform the data controller whether the application is accepted within seven (7) business days.
3. The national CAC will complete the security assessment within forty-five (45) business days (unless an extension of time is required for complicated situations).

Thus, the CAC approval process alone can take up to at least fifty-seven (57) business days, not including the time taken for self-assessment.

Validity of Security Assessment

Each security assessment is valid for two years from the date when the assessment result is released. If there is any significant change, the data controller shall reapply for a security assessment. If the cross-border data transfer activities will take more than two years, the data controller should resubmit for security assessment at least 60 business days before the expiry of the two-year validity period.

Cross-border Data Transfer Contract

The Measures require that each submission for a security assessment should include the agreement or legal document entered into by the data controller with the foreign data recipient which sets out, amongst other things:-

1. The purpose, method and scope of the data transfer;
2. The manner of overseas storage of data;
3. The obligations and liabilities of the foreign data recipient; and
4. The dispute resolution mechanism.

The Measures places an obligation on the foreign data recipient to take safety measures when there are force majeure events or changes in the data security regulation in the foreign location.

CAC advises that parties should pass the security assessment before signing contracts, and, alternatively, parties should provide that the contracts are subject to successful passing of the security assessment.

Chinese Standard Contractual Clauses for Cross-border Personal Information Transfer (the "Chinese SCCs")

Under the PIPL, standard contractual clauses prescribed by the Chinese government (the Chinese SCCs) can be used as the third of the three specified mechanisms for cross-border data transfers from China. The Chinese SCCs are provisions to be entered into by the companies (data controllers) and the overseas data recipients, governing the rights and liabilities of the companies, the overseas data recipients and individuals when the companies transfer personal data of the individuals to the overseas data recipients. Contracts between the companies and the overseas data recipients concerning the cross-border transfer of personal information may not conflict with the Chinese SCCs.

Who may use the Chinese SCCs?

Only companies which meet all of the following conditions may rely on the Chinese SCCs to transfer personal information outside of China:

1. It is not a CII Operator;
2. It processes personal information of less than one (1) million individuals;
3. It has not cumulatively provided overseas personal information of more than 100,000 individuals since 1 January of the preceding year; and
4. It has not cumulatively provided overseas sensitive personal information of more than 10,000 individuals since 1 January of the preceding year.

Impact assessment and recordal

The Chinese SCCs highlight the existing requirement that companies conduct impact assessments prior to transferring personal data cross-border, requiring that the companies submit both the impact assessment results and the Chinese SCCs to the local provincial level cyberspace authorities within ten (10) working days from the effective date of the Chinese SCCs. Impact results are required to be kept for at least three years, and this is also reiterated in the Chinese SCCs.

Where there is any change of circumstances, the Chinese SCCs should be re-executed and re-recordal is needed.

Rights of individuals

The Chinese SCCs require that the company notify the individual of it being a third party beneficiary under the Chinese SCCs, and the Chinese SCCs need to be provided to the individual upon request.

Where the overseas data recipient anonymises or deletes the personal data, it is required to provide an audited report to the individual.

The Chinese SCCs also reiterate various requirements already set out in the PIPL, including those in respect of automated decision making and transparency whereby the company and the overseas recipient need to explain the rules of data processing to the individual. Communications with the individual should be clear, easy to understand and thorough.

The Chinese SCCs also reiterate the individual's right to access, copy, amend and delete his/her data. If the individual's request is denied, they should be given reasons and informed of complaint and litigation options.

Audit

The Chinese SCCs provide that the individual may audit the data processing of the overseas recipient and the overseas recipient should facilitate such activities, including providing information relating to its qualification for data processing. The overseas data recipient must keep records of its data processing for at least three years.

Onward transfer of personal data

The onward transfer of personal data by the overseas recipient needs to meet additional requirements, such as meeting the necessity requirement and obtaining an additional consent (termed 'Separate Consent') from the individual.

Country risk assessment

Similar to the European situation, the Chinese SCCs also consider whether the jurisdiction of the overseas recipient accords a level of protection essentially equivalent to that required by the PIPL. The company and the overseas recipient need to conduct prior assessment, among other things, of the law for protection for personal information in the overseas jurisdiction.

Contact person

The overseas recipient should designate an internal contact for addressing inquiries and complaints from the individuals and the contact details should be notified to the individuals.

Governing law and dispute resolution

The governing law of the Chinese SCCs is, unsurprisingly, Chinese law. Disputes arising under the Chinese SCCs may be handled by arbitration or by litigation. Where arbitration is selected, it should be conducted by arbitration bodies in China or those under the New York Convention (Convention on the Recognition and Enforcement of Foreign Arbitral Awards). Where disputes are handled by litigation it shall be conducted in a Chinese court.

The individual is able to lodge complaints with Chinese regulators and/or sue in China, and the company and the overseas recipient are jointly liable to the individual under the Chinese SCCs.

Cataloguing of Important Data

The term “Important Data” was first mentioned in the China Cybersecurity Law, requiring that personal information and Important Data gathered or created by CII Operators during operations in China be stored in China. However, the term was not defined in that Law.

Draft regulations entitled Information Security Technology - Identification Guide of Important Data and Information Security Technology - Identification Rules of Important Data (which was not publicly released) set out different definitions of “Important Data”. The latest draft regulation, which is subject to further review and amendment, provides a significantly wider definition of “Important Data” than those in previous draft regulations. It provides that Important Data is “data that are domain-specific, group-specific, region-specific, or of a certain precision and scale, where national security, economy, social stability, public health or safety would be directly harmed in the event that the data are leaked, tampered with, or destroyed”. This definition is similar to that for Important Data in the Measures on Security Assessment of Cross-border Data Transfer released on 7 July 2022 and to be effective on 1 September 2022.

Cataloguing Principles and Factors

The draft regulation provides basic principles when cataloguing Important Data, which include:-

1. Focusing on impact on security: considering from the perspective of national security, economy stability, social stability, public health and safety. Data which are only important and sensitive to an organisation (e.g. data in relation to the internal management of a company) would not be deemed Important Data.
2. Highlighting the focus of data protection and facilitating the free flow of data (after ensuring security).
3. Linking up existing local rules.
4. Evaluating risks holistically.
5. Using both quantitative and qualitative methods.
6. Constant evaluation.

The draft regulation also lists a number of factors as examples to be taken into account when cataloguing Important Data. Important Data can be classified as data that may influence:-

1. National politics;
2. Sovereignty;
3. Military;
4. Economy;
5. Culture;
6. Society;
7. Technology;
8. Environment;
9. Resources;
10. Nuclear equipment;
11. Overseas interests;
12. Biology;
13. Outer space;
14. Polar region; or
15. Deep-water.

Data Classification and grading system

Important Data represents one grade (level 2) under the data classification and grading system under the Network Security Standard Practice Guide - Guidelines for Data Classification and Grading issued by the National Information Security Standardisation Technical Committee on 31 December 2021:

	IMPACTED SUBJECTS			
	NATIONAL SECURITY	PUBLIC INTERESTS	PERSONAL LAWFUL INTERESTS	ORGANISATIONAL LAWFUL INTERESTS
CORE DATA	Harm or significantly harm	Significantly harm	-	-
IMPORTANT DATA	Slightly harm	Harm or slightly harm	-	-
GENERAL DATA	No harm	No harm	No harm, slightly harm, harm, significantly harm	No harm, slightly harm, harm, significantly harm

Concluding Remarks

International businesses operating in and servicing China's large domestic market depend on the ability to store and process data, often requiring that data to be transferred across international borders. China continues to progress with increased protection of cyber security, data security and personal information, and whilst these new regulatory releases provide some welcome clarity to businesses on key areas such as the prescribed volume of data transfer without needing government approval and the process for obtaining government approval, there remains uncertainty around the wide definition of "Important Data". Irrespective of the questions that remain around China's cybersecurity regulations, businesses engaged in cross-border business need to be ready to comply with these latest releases. Businesses should thoroughly evaluate their data export activities and ensure that they are well positioned to implement necessary and adequate measures to comply with their responsibilities under the law.

The British Chamber of Commerce in China would like to thank PwC China and Tiang & Partners for their contribution to the article.

About British Chamber of Commerce in China

The British Chamber of Commerce in China is a membership organisation with a focus on providing advocacy, business support and networking opportunities for British businesses in China. We operate as an independent, not-for-profit organisation with a strong and diverse membership, representing British companies across the country from our office in Beijing and our broader network across Shanghai, Guangdong and Southwest China. With decades' worth of business experience in China, we bring the British business community together and help them thrive in one of the world's fastest growing market

BRITISH CHAMBER OF COMMERCE IN CHINA 中国英国商会