Technology, Data Protection & Cybersecurity

Special Edition

Cross-border Data Transfer Regulation Developments in China

Dedicated to Excellence

杰出 所以你安心

Beijing – Shanghai – Shenzhen – Hong Kong – Haikou – Nanjing

AnJie Broad
安杰世泽

Partner, AnJie Broad Law Firm
M +86 139 1067 7369
T +86 10 8567 2968
E: yanghongquan@anjielaw.com

19/F, Tower D1,
Liangmaqiao Diplomatic Office Building,
19 Dongfangdonglu,
Chaoyang District,
Beijing 100600, China

Dear Colleagues,

The past month has been a busy time for everyone. As you may have heard by now, the Cyberspace Administration of China ("**CAC**") and others have recently issued a series of regulations, draft regulations and guidelines that will change the cross-border data transfer environment in China.

As a result of these new regulations, we have received many enquiries from clients, who wish to know how the new regulations will affect their business.

Therefore, with a view to keeping our key clients informed about the changing regulatory environment, we have put together this special edition on the new developments of Chinese outbound data transfer legal regime for you.

This special edition will provide readers with an overview of the recent changes taking place in relation to Chinese cross-border data transfer regulation. It deals with the following different legal mechanisms for cross-border data transfers:

- Cross-border data transfer security assessments by the CAC;
- Standard Contracts for cross-border data transfers; and
- Certification for cross-border data transfers.

I hope that you find this special edition helpful.

Please feel free to get in touch with me if you have any questions.

Yours faithfully,

Samuel Yang

Samuel Yang

ANJIE BROAD LAW FIRM | Partner

Contents

China Issues Cross-border Data Transfer Security Assessment Rules 5
Purpose and Scope – Articles 1 & 2 5
Important Data – Article 19 6
Security Assessment Triggers – Articles 4 & 14 6
Data Transfer Legal Documents – Article 9 7
Self-assessments – Article 5 7
Security Assessment Applications – Article 6 8
Security Assessments – Articles 3, 10, 8, 11 & 14 8
Security Assessment Timescales – Articles 7, 12 & 13 8
Confidentiality Obligations – Article 15 9
Liability – Articles 16, 17 & 18 9
Effective Date and Transitional Period – Article 20 9
Summary 9
China Releases Draft Standard Contract for Cross-border Data Transfers 10
Provisions on Standard Contract on the Export of Personal Information (Draft for Public Consultation) 10
Analysis of Articles 1 and 2: 10
Analysis of Article 3: 11
Analysis of Article 4: 11
Analysis of Article 5: 13
Analysis of Article 6: 14
Analysis of Article 7: 14
Analysis of Article 8: 15
Analysis of Article 9: 15
Analysis of Article 10: 15
Analysis of Article 11: 15
Analysis of Article 12: 16
Analysis of Article 13: 16
Cross-Border Data Transfers: A Comparison of the EU and Chinese Standard Contractual Clauses 17
Background 17
Note on the Terms Used 17
Use Scenarios 17
General Observations 18
Direct Comparison 18
Implications 24

Will China's New Certification Rules Be a Popular Legal Path for Outbound Data Transfers? 25
Background 25
TC260 Issues Rules for Legal Path 3 (Certification) 25
Applicability of the Specifications 26
Legally Binding Documents 26
Uniform Processing Rules 26
DPO 26
Personal Information Protection Organisation 27
Personal Information Protection Impact Assessments (PIPIAs) 27
Individual Rights 27
Obligations of the Parties to Cross-Border Data Transfers 27
Conclusions 28
Our Technology, Data Protection and Cybersecurity Practice 29

China Issues Cross-border Data Transfer Security Assessment Rules

On 7 July 2022, the Cyberspace Administration of China ("**CAC**") issued the Measures for the Security Assessment of Outbound Data Transfers ("**Measures**"), which will take effect on 1 September 2022. The Measures underwent three rounds of public consultation in 2017, 2019 and 2021 before they were finalised.

In its final form, the Measures contain 20 articles. We have identified 11 topics within the Measures that cover:

No.	Topic	Articles
1.	Purpose and scope	1 & 2
2.	Important data	19
3.	Security assessment triggers	4 & 14
4.	Data transfer legal documents	9
5.	Self-assessments	5
6.	Security assessment applications	6
7.	Security assessments	3, 8, 10, 11 & 14
8.	Security assessment timescales	7, 12 & 13
9.	Confidentiality obligations	15
10.	Liability	16, 17 & 18
11.	Effective date and transitional period	20

In the following, we shall discuss each of the topics that we have identified in turn.

Purpose and Scope – Articles 1 & 2

The stated purpose of the Measures is "*to regulate outbound data transfer activities, protect personal information rights and interests, protect national security and social and public interests, and promote a safe and free flow of data across borders*" (Article 1).

Article 2 goes on to state that the measures apply to security assessments of outbound data transfers involving important data and personal information collected and generated by data processors through their operations in China. Based on Article 2, it seems that the Measures do not apply to personal information collected and generated by data processors from outside of China.

Important Data – Article 19

The Measures contain a definition of important data in the context of outbound data transfers. Important data is a nebulous concept in Chinese laws and regulations which requires further elaboration by the CAC and relevant industry regulators. For now, the term has only been further defined in the field of automotive data and in a few draft regulations. Below we compare the definition in the Measures with the core of the definition in the Several Provisions on Vehicle Data Security Management (Trial) ("**Trial Provisions**").

Measures for the Security Assessment of Outbound Data Transfers	**Several Provisions on Vehicle Data Security Management (Trial)**	**Comments**
For the purposes of these Measures, the term "important data" means any data, the tampering, damage, leakage, or illegal acquisition or use of which, if it happens, may endanger national security, the **operation of the economy, social stability, public health and security**, etc.	The term "important data" refers to any data that, once tampered with, sabotaged, leaked or illegally obtained or used, may lead to endangerment of national security **or public interests, or infringement of the lawful rights and interests of an individual or organisation**, including the following data: [Examples omitted]	Both definitions are risk-based, though the consequences that they consider differ slightly. We have made bold the more significant differences. As the CAC was involved in the preparation of both regulations, the differences suggest that the definition of important data will generally be: data that, if breached, may endanger the interests of the nation, public or persons.

Security Assessment Triggers – Articles 4 & 14

An entity must declare intended outbound data transfers by a data processor to provincial CACs and seek security assessments if the data processor:

1) intends to transfer important data;
2) is a Critical Information Infrastructure operator ("**CIIO**") intending to transfer personal information;
3) is a personal information processor who has processed the personal information of over 1 million people;
4) has cumulatively made outbound transfers of the personal information of over 100 thousand people since 1 January of the previous year;
5) has cumulatively made outbound transfers of the sensitive personal information of over 10 thousand people since 1 January of the previous year; and
6) falls within other situations prescribed by the CAC.

Whether companies will be regarded as CIIOs remain unclear in many industries. Despite the uncertainty in existing and future regulations, a more straightforward judgement would be that a company is not a CIIO unless it has been notified by a competent authority that it has been identified as a CIIO.

It is understood that many companies would prefer to see a rise in the threshold transfer volumes of personal information that trigger security assessments.

Security assessments can also be retriggered in one of the following circumstances:

1) there is a change in the particulars of processing by the overseas recipient, which will affect the security of the data, or the period for retaining data is to be extended;
2) there is any change in the data security protection policies and legislation and cybersecurity environment, or a force majeure event occurs where the overseas recipient is located,

3) there is a change in the actual control of the data processor or overseas recipient or any change to the data transfer agreement, which will affect the security of the outbound data; or
4) any other circumstance exists that may affect the security of the data.

Data Transfer Legal Documents – Article 9

The Measures state that the legal documents between the data exporter and data importer for outbound data transfers should cover:

1) the purpose and method of the outbound data transfer, the scope of data, and the purpose and method of the data processing;
2) the data retention place and period, and obligations when the retention period expires, the transfer purpose completes, or the agreement is terminated;
3) restrictions against onwards transfers of outbound data to others;
4) security measures to be adopted when material changes occur in relation to the overseas recipient, the legal, regulatory environment and cybersecurity environment of the destination country, or a force majeure event occurs that makes it difficult to ensure data security;
5) remedial measures, liability for breach of contract and dispute resolution in the event data security protection obligations are breached; and
6) requirements for proper emergency disposal and ensuring the channels and ways for individuals to safeguard their personal information rights and interest when data is exposed to the risk of security breaches.

On a related note, the CAC also issued the Draft Provisions on Standard Contracts for the Export of Personal Information on 30 July 2022, which also deal with outbound data transfers and contains a draft Standard Contract that was prepared for use in situations that would not trigger the security assessments under the Measures. While they certainly have some similarities, companies should not assume that signing the Standard Contract would meet the requirements in the Measures.

Self-assessments – Article 5

After a security assessment is triggered, but before a security assessment application is made, a data processor should conduct a self-assessment. Data processors need to address the following factors during self-assessments:

1) the legality, legitimacy and necessity of the transfer and the purpose, scope and manner of data processing by the overseas recipient;
2) the quantity, scope, type and sensitivity of the outbound data, and the risks the outbound data might pose to national security, public interests, and the lawful rights and interests of individuals and organisations;
3) whether the responsibilities and obligations undertaken by the overseas recipient and the management and technical measures and capabilities of the overseas recipient to perform such responsibilities and obligations can ensure the security of the outbound data;
4) the risk of the outbound data suffering from data breaches, including unauthorised onward transfers, during and after the outbound data transfer, and whether individuals have smooth channels to safeguard their rights and interests in their personal information and other data;
5) whether data security protection responsibilities and obligations are sufficiently stipulated in the data transfer agreement or other documents; and
6) other matters that may affect the security of the outbound data transfer.

Some of the factors described above are also subjects of the personal information protection impact assessment ("**PIPIA**") required under the Personal Information Protection Law ("**PIPL**"). We believe it would be cost-effective for companies to consider all assessment factors under both the PIPL and the Measures and make one consolidated self-assessment.

Security Assessment Applications – Article 6

Applications for security assessments should contain:

1) an application form;
2) a self-assessment report;
3) a copy of the outbound data transfer agreement; and
4) other materials required by the CAC.

Security Assessments – Articles 3, 10, 8, 11 & 14

According to Article 3 of the Measure, a security assessment of outbound data transfers should combine ex-ante assessment and ongoing supervision and self-assessment and security assessment.

The substantive content of a security assessment by the CAC overlaps significantly with the above-mentioned self-assessments, except for the following matters:

1) the impact of data security protection policies and legislation and the cybersecurity environment of the country or region where the overseas recipient is located on the security of the outbound data; whether the data protection level of the overseas recipient meets the requirements of Chinese laws and administrative regulations and the mandatory national standards;
2) the compliance with China's laws, administrative regulations and departmental rules; and
3) other matters to be assessed the CAC deems necessary.

We note that item 1) above seems to describe something which is similar to the "transfer impact assessment" in the EU and that data processors are not expected to cover such things in their self-assessment report. As government departments have limited resources, we doubt that they will make such assessments on a case-by-case basis. Accordingly, we wonder whether a central transfer impact assessment list exists at this time, whether it will become accessible in the future, and how it will be managed and updated.

The CAC can terminate security assessments if the CAC requires additional materials and a data processor refuses to submit them.

Under Article 14, the results of a security assessment are valid for two years unless a retriggering event occurs. Data processors will need to apply for a reassessment after expiration.

Security Assessment Timescales – Articles 7, 12 & 13

Security assessment applications need to be submitted to the relevant provincial CAC, which should confirm the completeness of documents within a maximum of 5 working days. Then the application documents will be provided to the central CAC who may take up to 7 working days to determine whether to accept the application for a substantive review, which should take a maximum of 45 working days from the date of issuing a written acceptance of the application. Accordingly, in normal circumstances, the entire process of applying for and undergoing a security assessment might take up to 57 working days (approximately 2.5 months).

However, the Measures allow the CAC to extend the deadline for completing a security assessment "*as appropriate*" if the "*case is complicated or there are materials to be supplemented or corrected…*"

If a data processor objects to the assessment results, it should apply for a reassessment within 14 working days of the receipt of the assessment results. According to Article 15, the results of a reassessment are final.

Confidentiality Obligations – Article 15

Institutions and staff that participate in security assessments must keep confidential, as required by law, any information that they learn during their work. This includes any state secret, personal privacy, personal information, trade secret, confidential business information, and other data.

Liability – Articles 16, 17 & 18

Any person may report violations of the Measures to the CAC.

If the CAC discovers outbound data transfers that have passed a security assessment no longer conform to the Measures during the implementation of data transfers, it may notify the data processor to terminate such transfers. If the data processor needs to continue making such transfers, it should make "*rectification as required*" before applying for a reassessment. The full implications of this are unclear at this time, but it suggests that the CAC may eventually interpret or construe data transfer agreements and decide whether they are being properly performed, or they might attach conditions to the transfers following their assessments or both.

Violations are to be dealt with under the Cybersecurity Law, the Data Security Law or the PIPL, and other laws and regulations depending on the data processor, the data and the nature of the violation. We note that violations of the PIPL may attract the highest penalties, specifically, up to CNY 50 million or 5% of the violator's revenue in the previous year.

Effective Date and Transitional Period – Article 20

The Measures take effect on 1 September 2022. This means that any relevant outbound transfers from 1 September 2022 should only be carried out after data processors have passed security assessments. For outbound data transfers carried out before 1 September 2022, "rectification" shall be completed within 6 months after 1 September 2022. It is unclear if this means that the data processor must pass the security assessment within this 6-month grace period, or perhaps the submission of an application for security assessment within this period would be sufficient. Nevertheless, given these deadlines, possible delays, the 2022 spring festival holidays and other factors, we recommend that data processors should endeavour to submit their applications for security assessments as soon as possible.

Summary

The requirements for security assessment apparently add a layer of onerous compliance burdens to the operations of many businesses. The various thresholds of personal information that trigger security assessments are low and may affect many multinational companies doing business in China. These new requirements also create some uncertainty, particularly among entities that depend on cross-border transfers of data to conduct business. This uncertainty will not be resolved until the Measures take full effect and the processing of security assessments becomes standardised in practice.

Businesses that will likely be subject to the security assessment regime should act now - take stock of their data flows, renegotiate their cross-border data transfer contracts and ensure that their data protection practices align with the requirements of the Measures and other Chinese laws and regulations. Businesses that operate in areas of higher risk may also wish to begin creating contingency plans in case they are prohibited from transferring certain data out of China.

China Releases Draft Standard Contract for Cross-border Data Transfers

On 30 June 2022, the Cyberspace Administration of China ("**State Internet Information Department**" or "**CAC**") issued the Draft Provisions on Standard Contracts for the Export of Personal Information ("**Draft Provisions**") for public consultation. The deadline for feedback is 29 July 2022.

The Draft Provisions contain a draft Standard Contract for the Export of Personal Information ("**Standard Contract**"). The Standard Contract consists of nine articles and two appendices.

This article provides an in-depth analysis of the articles in the Draft Provisions and their potential impact on multinational companies.

Provisions on Standard Contract on the Export of Personal Information (Draft for Public Consultation)

Article 1: These Provisions are formulated on the basis of the "Personal Information Protection Law of the People's Republic of China" so as to standardise personal information export activities, protect personal information rights and interests, and promote the safe and free flow of personal information across borders.

Article 2: Where personal information processors conclude contracts with overseas recipients to provide personal information outside the territory of the People's Republic of China in accordance with subparagraph (3) of the first paragraph of Article 38 of the "Personal Information Protection Law of the People's Republic of China", they shall follow these Provisions to sign a standard contract for the export of personal information (hereinafter referred to as "**Standard Contracts**"). Other contracts concluded between the personal information processor and the overseas recipient related to the outbound activities of the personal information shall not conflict with the standard contract.

Analysis of Articles 1 and 2:

1. Articles 1 and 2 explain the purpose and legal basis for formulating the Draft.
2. Article 2 provides:

   "Other contracts concluded between a personal information processor and an overseas recipient related to the outbound activities of personal information must not conflict with the Standard Contract."

3. This means that, in addition to signing the Standard Contract with an overseas recipient, a Chinese enterprise that chooses to use a Standard Contract also needs to:

   a) check other contracts it has signed with the overseas recipient related to the export of personal information to ensure that they do not conflict with the Standard Contract, and supplement or modify such other contracts according to the actual situation; and
   b) clearly state in other contracts that in the event of a conflict with the terms of the Standard Contract, the Standard Contract prevails.

Article 3: Those carrying out personal information export activities on the basis of standard contracts shall adhere to a combination of independent contracting with file management to prevent security risks to the export of personal information and ensure the orderly and free flow of personal information in accordance with the law.

Analysis of Article 3:

1. According to the expression "*independent contracting*" in Article 3, signing a Standard Contract is not a mandatory legal obligation. However, enterprises should note that for all data export paths permitted under Article 38 of the Personal Information Protection Law ("**PIPL**"), Chinese enterprises and overseas recipients must either sign (i) Standard Contracts, (ii) other similar contracts or (iii) legally binding and enforceable documents. See our analysis of Articles 4 and 5 below for details.
2. For the "*file management*" requirement, see our analysis of Article 7 below.

Article 4: Where personal information processors meet all the following criteria, they may provide personal information overseas by signing a standard contract:

(1) Non-critical information infrastructure operators;

(2) Handling less than 1 million persons' personal information;

(3) Cumulative provision of personal information of less than 100,000 people overseas since 1 January of the previous year;

(4) Cumulative provision of sensitive personal information of less than 10,000 people outside the country since 1 January of the previous year.

Analysis of Article 4:

4. Under Article 4, a processor of personal information who meets the relevant requirements **"may"**, as opposed to "**must**", sign a Standard Contract to legalise the export of personal information. This is because Article 38 of the PIPL stipulates several different legal paths for personal information to leave China. They include:

> *(1) Critical information infrastructure operators and personal information processors handling personal information that reach the number of personal information processors provided for by the state network information departments for outbound conduct shall pass a security assessment organised by the state network information departments;*
> *(2) Conduct personal information protection certification through professional bodies in accordance with the provisions of the state network information departments;*
> *(3) Conclude a contract with an overseas recipient in accordance with a standard contract formulated by the State Internet Information Department, stipulating the rights and obligations of both parties;*
> *(4) Other requirements provided for by laws, administrative regulations, or the State Network Information Department.*

5. According to the above provisions, Chinese enterprises that are not "*critical information infrastructure operators and personal information processors who process personal information to the amount prescribed by the State Internet Information Department*" may (i) sign the Standard Contract or (ii) obtain personal information protection certification through a professional body to transfer personal information overseas.
6. Therefore, for Chinese enterprises that choose path (ii), signing a Standard Contract is not required. However, it should be noted that although a Chinese enterprise that chooses path (ii) does not need to sign a Standard Contract, it will still need to sign a "*legally binding and enforceable document*" with the overseas recipient in accordance with the Technical Specification for the Certification of Cross-border Processing Activities of Personal Information, which was officially issued by the National Information Security Standardization Technical Committee (also known as TC260) on 24 June 2022. Such a document should at least specify the following:

> *a) Personal data processors and overseas recipients carrying out cross-border personal information processing activities;*

b) The purpose of cross-border processing of personal information and the types and scope of personal information;
c) Measures to protect the rights and interests of Personal Information Subjects;
d) The overseas recipient undertakes to comply with the unified rules for the cross-border handling of personal information, and ensures that the level of personal information protection is not lower than the standards stipulated by the relevant laws and administrative regulations of the People's Republic of China on the protection of personal information;
e) The overseas recipient undertakes to accept the supervision of the certification body:
f) The overseas recipient undertakes to accept the jurisdiction of the laws and administrative regulations of the People's Republic of China on the protection of personal information;
g) Clearly define the organisations that bear legal responsibility within the territory of the People's Republic of China:
h) Other obligations stipulated by laws and administrative regulations that shall be observed.

7. Article 4 clearly restricts the application of Standard Contracts and prohibits their use in circumstances where:

    a) Critical information infrastructure operators export personal information;
    b) Personal information processors have processed the personal information of more than 1 million people;
    c) The cumulative export of personal information exceeds 100,000 people since 1 January of the previous year; and
    d) The cumulative export of sensitive personal information exceeds 10,000 people since 1 January of the previous year.

8. Those circumstances are the personal information export activities of "*critical information infrastructure operators and personal information processors who handle the number of personal information specified by the state network information department*", as stated in Articles 38 and 40 of the PIPL. Such transfers should be preceded by an application for a Security Assessment under the Measures for Security Assessment of Data Export (Draft) (29 October 2021) rather than the signing of a Standard Contract.
9. Several categories of Chinese enterprises that should apply for security assessments do not need to legalise their personal information exports by signing a Standard Contract. Instead, and according to the Measures for Security Assessment of Data Export (Draft for Comments), they should sign a contract with the overseas recipient that includes but is not limited to the following:

    (1) The purpose, method, and scope of data exported, and the purpose and method of processing data by overseas recipients;
    (2) The place and period of time for which the data is kept overseas, as well as measures for handling outbound data after the retention period is reached, the agreed purpose is completed, or the contract is terminated;
    (3) Restrictive clauses restricting overseas recipients from transferring outbound data to other organisations or individuals;
    (4) The security measures that the overseas recipient shall adopt when there is a substantial change in its actual control or business scope, or when the legal environment of the country or region in which it is located makes it difficult to ensure data security;
    (5) Liability for breach of contract and binding and enforceable dispute resolution clauses for breach of data security protection obligations;
    (6) When risks such as data leakage occur, properly carry out emergency response, and ensure smooth channels for individuals to safeguard personal information rights and interests.

10. Article 4 is also consistent with Article 38 of the PIPL, which only stipulates that "*personal information processors*" may sign the "*Standard Contract*". However, it does not explicitly address whether "*entrusted processors*" under the PIPL can or should sign the Standard Contract. For readers more familiar with the GDPR, "*personal information processors*" are roughly equivalent to data controllers, while the concept of "*entrusted processors*" is roughly equivalent to data processors.
11. In serving clients, we have observed that some business models involve data transfers from (i) a Chinese personal information processor to (ii) a domestic entrusted processor to (iii) an overseas sub-processor. Domestic personal information processors and domestic entrusted processors often disagree over which party should sign the Standard Contract with the overseas sub-processor.

12. We believe domestic personal information processors should usually bear the primary obligation for signing a Standard Contract containing a clear mechanism describing the parties' obligations and responsibilities with an overseas subcontractor to enable a domestic entrusted processor to provide data to said overseas subcontractor.
13. An alternative approach would be for a domestic personal information processor, domestic entrusted processor and overseas subcontractor to sign a tripartite Standard Contract. However, this would require further clarity regarding the mechanism for domestic entrusted processors to provide data to overseas subcontractors and each party's contractual obligations and responsibilities.

Article 5: Before personal information processors provide personal information overseas, they shall carry out a personal information protection impact assessment in advance, focusing on the following content:

(1) The legality, legitimacy, and necessity of the purpose, scope, and methods of processing personal information by personal information processors and overseas recipients;

(2) The quantity, scope, type, and sensitivity of outbound personal information, and the risks that personal information may bring to the rights and interests of personal information that may be brought about by the export of personal information;

(3) The responsibilities and obligations undertaken by the overseas recipient, as well as whether management and technical measures and capabilities for performing responsibilities and obligations can ensure the security of outbound personal information;

(4) The risk of personal information being leaked, damaged, altered, or abused after leaving the country, and whether the channels for individuals to safeguard personal information rights and interests are unobstructed, and so forth;

(5) The impact of personal information protection policies and regulations on the performance of standard contracts in the country or region where the overseas recipient is located;

(6) Other matters that might affect the security of personal information leaving the country.

Analysis of Article 5:

1. Article 5 refines the requirements for personal information protection impact assessments before exporting personal information under the PIPL by providing additional detail and specification.
2. It is worth noting that Chinese enterprises need to assess "*the impact of personal information protection policies and regulations of the country or region where the overseas recipient is located on the performance of standard contracts*", which is not a small task. Going forward, Chinese enterprises will need to rely more heavily on advice from overseas legal professionals and assistance from overseas recipients.

Article 6: The standard contract includes the following main contents:

(1) Basic information of personal information processors and overseas recipients, including but not limited to names, addresses, contact names, contact information, and so forth;

(2) The purpose, scope, type, sensitivity, quantity, method, retention period, storage location, and so forth of personal information exported;

(3) The responsibilities and obligations of personal information processors and overseas recipients to protect personal information, as well as technical and management measures adopted to prevent security risks that may arise from leaving the country;

(4) The impact of the personal information protection policies and regulations of the country or region where the overseas recipient is located on compliance with the terms of this contract;

(5) Personal Information Subjects' rights, as well as channels and methods for safeguarding Personal Information Subjects' rights;

(6) Relief, contract rescission, liability for breach of contract, dispute resolution, etc.

Analysis of Article 6:

1. Article 6 provides an overview of the Standard Contract. Regarding the specific content of the Standard Contract, we will analyse and interpret it separately.

Article 7: Personal information processors shall file a record with the provincial-level internet information department for the area where they are located within 10 working days of the standard contract taking effect. The following materials shall be submitted for filing:

(1) standard contracts;

(2) personal information protection impact assessment reports.

The personal information processor is responsible for the authenticity of the materials filed. After the standard contract takes effect, the personal information processor may carry out personal information export activities.

Analysis of Article 7:

1. The Article 7 filing provisions are new legal requirements without any precedent in the PIPL. The Standard Contract and the personal information protection impact assessment report on the export of personal information will need to be filed with the government.
2. Considering that many enterprises will need to make filings, national administrative resources are limited, and other factors, filing management within provincial CACs may only consist of formality reviews. Based on informatisation trends in China, the CAC may establish an online filing system to facilitate filings.

Article 8: Where any of the following circumstances occur during the validity period of a standard contract, the personal information processor shall re-sign the standard contract and file it for the record:

(1) Where the purpose, scope, type, sensitivity, quantity, method, retention period, storage location, and purpose or method of handling personal information handled by overseas recipients change, or extend the period for personal information to be retained abroad;

(2) Where changes in personal information protection policies and regulations in the country or region where the overseas recipient is located may affect personal information rights and interests;

(3) Other circumstances that might affect the rights and interests of personal information.

Analysis of Article 8:

1. Considering the requirements of Articles 5 and 6 above, the content of Article 8 seems reasonable at face value.
2. However, determining whether the "*personal information protection policies and regulations of the country or region where the overseas recipient is located*" has "*changed*" and "*may affect the rights and interests of personal information*" is a big challenge for even the largest multinational enterprises. It seems that Chinese enterprises will be expected to keep abreast of changes in policies and regulations related to overseas personal information protection. This may require them to retain overseas legal professionals on an ongoing basis.

Article 9: Institutions and personnel participating in the filing of standard contracts shall preserve the confidentiality of personal privacy, personal information, commercial secrets, confidential business information, and so forth that they learn of in the course of performing their duties, and must not leak or illegally provide or use them to others.

Analysis of Article 9:

1. Some enterprises, especially multinational enterprises, may have concerns about whether the Standard Contract and the personal information protection impact assessment report filing mechanism may cause information leakages. Article 9 seems to be an attempt to pre-empt such concerns.
2. The expression "*confidential business information*" has also appeared in the Measures for the Security Assessment of Data Export (Draft for Public Consultation). How the CAC will define it in practice remains to be seen.

Article 10: Where any organisation or individual discovers that a person handling personal information has violated these Provisions, they have the right to make a complaint or report to the provincial level Internet information department.

Analysis of Article 10:

1. Complaints and reports may come from a personal information processor's (possibly disgruntled) employees or Personal Information Subjects.
2. We speculate that, in the future, the CAC could publish lists of enterprises that have completed the filing procedures and that Personal Information Subjects could use such lists to determine whether a personal information processor has fulfilled its filing obligations to make targeted reports.

Article 11: Where provincial-level Internet information departments discover that personal information outbound activities through the signing of standard contracts no longer meet the requirements for security management of personal information export in the course of actual processing, they shall notify the personal information processors in writing to terminate personal information export activities. Personal information processors shall immediately terminate personal information export activities upon receipt of the notice.

Analysis of Article 11:

1. As mentioned above, many enterprises may need to make filings, and state resources are limited. As such, filing management by the CAC may only consist of a formality review. However, given the content of Article 11, provincial-level CACs may also adopt methods such as spot checks, focusing on specific enterprises or industries

and making investigations based on whistle-blowing leads to conduct targeted substantive reviews of outbound personal information transfers.

Article 12: Where personal information processors follow these Provisions to conclude standard contracts with overseas recipients to provide personal information overseas, and any of the following circumstances occur, the provincial-level Internet information department is to follow the provisions of the "Personal Information Protection Law of the People's Republic of China" to order corrections within a time limit; Where they refuse to make corrections or harm the rights and interests of personal information, order them to stop activities of exporting personal information, and punish them in accordance with law; Where a crime is constituted, criminal responsibility is to be pursued in accordance with law.

(1) Failing to perform filing procedures or submitting false materials for filing;

(2) Failing to perform the responsibilities and obligations stipulated in the standard contract, infringing on the rights and interests of personal information, causing harm;

(3) Other circumstances affecting the rights and interests of personal information arise.

Analysis of Article 12:

1. It is worth noting that a "*failure to sign the Standard Contract*" is not a violation of these Provisions. However, as discussed above, the legal paths for exporting personal information are limited to those stipulated in Article 38 of the PIPL, which are:

   (1) Critical information infrastructure operators and personal information processors handling personal information that reach the number of personal information processors provided for by the state network information departments for outbound conduct shall pass a security assessment organised by the state network information departments;
   (2) Conduct personal information protection certification through professional bodies in accordance with the provisions of the state network information departments;
   (3) Conclude a contract with an overseas recipient in accordance with a standard contract formulated by the State Internet Information Department, stipulating the rights and obligations of both parties;
   (4) Other requirements provided for by laws, administrative regulations, or the State Network Information Department.
2. If a Chinese enterprise fails to sign a Standard Contract and fails to meet the requirements of other personal information export routes, it will not be punished for violating the provisions of Article 12. However, it will have violated Article 38 of the PIPL and may need to bear legal liability.

Article 13: These Provisions shall take effect as of _____

Analysis of Article 13:

1. We hope that when the CAC issues the final version of the above provisions, it will fully consider the time required for enterprises to comply with the new regulations (legal analysis, translation, negotiation with overseas recipients, etc.) and provide a reasonable time for enterprises to comply before the official implementation date.

Cross-Border Data Transfers: A Comparison of the EU and Chinese Standard Contractual Clauses

Background

On 30 June 2022, the Cyberspace Administration of China ("**CAC**") issued the Draft Provisions on Standard Contracts for the Export of Personal Information ("**Draft Provisions**") for public consultation. The Draft Provisions open a lawful path for cross-border data transfers under Article 38 of the Personal Information Protection Law ("**PIPL**"). The deadline for feedback is 29 July 2022.

The Draft Provisions contain a draft Standard Contract for the Export of Personal Information ("**PRC SCCs**"), which we shall compare in detail below to the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Regulation (EU) 2016/679 issued by the European Commission on 4 June 2021(those standard contractual clauses, the "**EU SCCs**"; and that regulation, the "**GDPR**").

Note on the Terms Used

We note that the lexicons used by the PIPL and GDPR vary somewhat. The terms we use to discuss the Chinese SCCs and EU SCCs (collectively or generally, "**SCCs**") reflect the terms used in the PIPL and GDPR, respectively. A table of equivalent concepts is provided below:

PIPL	**GDPR**
Personal Information Processor	Data Controller
Entrusted Processor*	Data Processor
Personal Information Protection Impact Assessment or PIPIA	Data Protection Impact Assessment or DPIA
Personal Information Subject	Data Subject
Sensitive Personal Information	Special Categories of Personal Data
Overseas Recipient	Data Importer
Regulator	Supervisory Authority

**This is a concept that can be understood in the context of Article 21 of the PIPL but is not explicitly defined in the PIPL.*

Use Scenarios

The PRC SCCs may only be used in the following relevant cross-border transfer scenarios:

(1) Non-critical information infrastructure operators;
(2) The Personal Information Processor has handled the personal information of less than 1 million people ;
(3) Since January 1 of the previous year, the cumulative amount of personal information provided overseas has not reached 100,000 people ;
(4) Since January 1 of the previous year, the cumulative amount of sensitive personal information provided overseas has not reached 10,000 people.

For more information about relevant cross-border data transfers, please see *"China Releases Draft Standard Contract for Cross-border Data Transfers."*

It is unclear if the PRC SCCs are customisable. However, Article 38 of the PIPL clearly states that contracts should be "*in compliance with the standard contract provided by the national cyberspace authority…*", which could mean that the PRC SCCs should remain unchanged and be used as an intact document.

General Observations

We note that the PRC SCCs consist of 9 articles and 2 appendices, while the EU SCCs consist of 18 clauses and 3 appendices. However, such a high-level comparison does not necessarily indicate the substance of either document.

The PRC SCCs can be considered a single document that applies to all relevant cross-border data transfers. They apply to all processors of personal information and do not define Entrusted Processors.

In contrast to the PRC SCCs, the EU SCCs can be considered 4 documents covering 4 different cross-border data transfer scenarios. Those transfer scenarios are: controller to controller; controller to processor; processor to processor; and processor to controller. Users of the EU SCCs require some familiarity with its layout as use requires the selection and deletion of clauses to match the transfer scenario.

Direct Comparison

We have produced the table below to help readers understand the structures of the PRC SCCs and EU SCCs. The table matches various topics identified within each document to specific provisions.

Topic	PIPL SCCs	GDPR SCCs	AnJie Broad's Comments
Definitions and interpretation.	Article 1	Clause 1. Clause 4.	The PRC SCCs provide 7 definitions and a catch-all. Some definitions refer directly to the PIPL, while others are China-specific. For instance, "*Relevant laws and regulations*" refers to Chinese laws and regulations only. While the EU SCCs lack a specific definitions section, Clause 1 therein contains some generic definitions found in most agreements, while Clause 4, an interpretation clause, refers readers to the GDPR for terms defined there. One thing to note is that Entrusted Processors, a concept that is defined in the context of Article 21 of the PIPL, are not described or referred to in the PRC SCCs. To express this in GDPR terms, the Chinese SCCs do not explicitly recognise the existence of Data Processors.
Sensitive personal information and special categories of personal data	Article 1.	Module One, Clause 8.6.	The EU SCCs provide an explicit definition without cross-references to the GDPR, while the PRC SCCs refer to the definition under the PIPL. We note that the relevant definitions under the PIPL and GDPR vary significantly, with the PIPL employing an open risk-based definition (PIPL, Article 28) and the GDPR employing what appears to be a very narrow and closed definition limited by examples. In practice, this means that sensitive personal information under the PRC SCCs will include other things that are not included in the EU SCCs. For instance, your bank details are not special categories of personal data under GDPR but would be sensitive personal information under the PIPL.

Transparency.	Article 2, Item 2	Module One, Clause 8.2. Module Two, Clause 8.3. Module Three, Clause 8.3.	The PRC SCCs require personal information processors to inform Personal Information Subjects about the particulars of all overseas recipients. In contrast, the EU SCCs only explicitly require Data Controllers to inform Data Subjects about the particulars of an overseas recipient where the said recipient is another Data Controller.
Data minimisation.	Article 2, Item 1.	Module One, Clause 8.2.	Under the PRC SCCs, the burden of ensuring data minimisation is on Personal Information Processors that act as transferors. In contrast, the EU SCCs appear to only burden Data Controllers that act as Data Importers. Placing the obligation on the party that initially controls that information seems to be a better way of controlling the risks associated with such transfers as a Data Importer cannot abuse data they lack. However, to manage this potential conflict in legal obligations, we imagine that, in the near future, many PRC-EU DPAs will include mutual commitments concerning data minimisation.
Personal Subject or Data Subject (collectively or generally, "Subject") rights.	Article 2, Item 3. Article 2, Item 8. Article 3, Item 2. Article 5. Article 6, Item 1.	Clause 3. Module One, Clause 8.3. Module Three, Clause 8.3. Clause 10.	Subject rights vary between the PRC and the EU. Additionally, Subject rights under the PRC SCCs are enforceable against both parties, while under the EU SCCs, the matter of enforceability depends on the nature of the underlying cross-border data transfer scenario. Both SCCs require a recipient to provide notices or information on its website detailing the contact details for a person who can handle inquiries and how enquiries should be handled. Both SCCs treat Subjects as third-party beneficiaries with a right to view the relevant SCCs. Moreover, both SCCs allow the principal contracting parties to charge fees or refuse to comply with unreasonable Subject requests.
Due diligence on the recipient.	Article 2, Item 4	Clause 8.	Personal Information Processors must, under the PRC SCCs, "*use reasonable efforts*" to ensure that "*the overseas recipient can fulfil its obligations*". Likewise, the EU SCCs require a Data Exporter to use "*reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations…*" The use of a reasonable efforts standard by both SCCs is interesting. We note that other parts of both SCCs stipulate best efforts standards, suggesting that the due diligence standards of care are lower than those for other matters.

Secure processing.	Article 2, Item 4. Article 3, Item 5.	Module One, Clause 8.5. Module Two, Clause 8.6. Module Three, Clause 8.6. Module Four, Clause 8.2.	Generally, the provisions of both SCCs aim to bring about the same or similar outcomes, namely appropriate technical and organisational measures. While the EU SCCs elaborate more on things that should be considered to bring about such outcomes, such additional details are arguably unnecessary. Concerning access controls, there appears to be broad equivalence between the SCCs. However, the PRC SCCs explicitly require Overseas Recipients to have "*a minimum authorised access control policy…*"
Provision of laws and technical standards.	Article 2, Item 5.	N/A	Personal Information Processors must provide Overseas Recipients with a copy of "*relevant legal provisions and technical standards*" upon request. This does not appear to have an equivalent within the GDPR. Should the exercise of such a right occur in practice, we imagine that foreign recipients might need translations. Procuring such translations, especially technical standards, could be expensive in practice. Contracting parties should consider this in their pricing and negotiations.
Cooperation with regulatory authorities and acceptance of their oversight.	Article 2, Item 6. Article 3, Item 12.	Module One, Clause 8.9. Clause 13.	Under the PRC SCCs, both contracting parties agree to respond to the Regulator's enquiries. Moreover, the Overseas Recipient must agree to cooperate with the Regulator's inspections, obey the Regulator and provide them with proof that "*necessary actions have been taken.*" We imagine the PRC SCCs could cause issues if EU blocking statutes exist (which we understand is the case). Under the EU SCCs, the Data Importer only agrees to make documents available to the Supervisory Authority. While this requirement is less onerous than that found under the PRC SCCs, we note that under the Data Security Law, Article 36, "*Any organisation or individual within the territory of the PRC shall not provide any foreign judicial body and law enforcement body with **any data** stored within the territory of the PRC without the approval of the competent authority of the PRC.*"
Impact assessment.	Article 2, Item 7. Article 4.	Clause 14.	The PRC and EU SCCs require a transferring party to conduct impact assessments for cross-border data transfers. Whilst the obligations of the SCCs do not wholly align, we believe that, in practice, a single assessment form or template could be used to ensure compliance with both sets of SCCs. As the GDPR and EU SCCs predate the PIPL and the PRC SCCs, we expect that many such forms or templates will likely be variations of styles used in the EU.
Compliance and record keeping.	Article 2, Item 9.	Module One, Clause 8.9.	Under the PRC SCCs, Personal Information Processors are burdened with proving that they have fulfilled their contractual obligation. In the case of disputes between the contractual parties, it is unclear if this would function as a

	Article 3, Item 10-12.	Module Two, Clause 8.9. Module Three, Clause 8.9. Module Four, 8.3	reverse burden of proof. However, such a reverse burden of proof could exist in disputes with Subjects. Overseas Recipients under the PRC SCCs must provide Personal Information Processors with evidence of their compliance, access to files and documents, facilitate audits, and accept the Regulator's supervision. Overseas recipients must retain their records for at least 3 years. Under the EU SCCs, obligations vary depending on the cross-border data transfer scenario, but in all cases involve being able to demonstrate compliance (sometimes to the other party) and making documents available to the regulator upon request. Modules Two to Four require recipients to facilitate audits and, for Modules Two and Three only, specify that audits may occur onsite.
Transfer particulars.	Article 3, Item 1. Appendix 1	Clause 6. Clause 8.1. Annex I. Annex II.	Both SCCs rely on an Appendix or Annex to state the particulars of a specific cross-border transfer. They are broadly comparable, except that the PRC SCCs require a clear statement on the quantity of personal information transferred and suggest using the personal information categories listed in recommended national standard GB/T35273.
Access by government authorities at destination.	Article 3, Item 7.	Clause 15.	The EU SCCs describe how to handle legally binding requests or demands from foreign authorities with jurisdiction over personal information in the destination country. This is a prudent measure to help entities manage conflicting legal systems. Unfortunately, the PRC SCCs contain no explicit provisions about dealing with legally-binding requests or demands from foreign authorities with jurisdiction over personal information in the destination country. We note that there is an express and general prohibition against providing "*personal information to third parties located outside the PRC.*" This could cause issues in practice and might deter entities from transferring their data abroad.
Data retention and deletion.	Article 3, Item 4. Appendix 1.	Module One, Clause 8.4. Module Two, Clause 8.5. Module Three, 8.5.	The provisions under both SCCs are broadly comparable with the exception that, under the PRC SCCs, an Entrusted Processor who is an Overseas Recipient must provide an audit report after deletion or anonymisation.
Data breaches.	Article 3, Item 6.	Module One, Clause 8.5.	Under the PRC SCCs, the requirements for handling all data breaches involve taking remedial measures, "*immediately*" notifying the Personal Information Processor and the Regulator, notifying Subjects if required by law, and documenting all facts about breaches. We do not believe that "*immediately*" is to be taken literally. However, some industries in China, such as insurance, have reporting

		Module Two, Clause 8.6. Module Three, Clause 8.6. Module Four, 8.2.	requirements that can be as short as one hour. As such, the meaning of immediately should not be assumed, and a service level agreement may be desirable for some industries. Obligations concerning data breaches under the EU SCCs can vary depending on the cross-border data transfer scenario and risk level. For instance, transfers between Data Controllers attract the most onerous obligations in the event of high-risk data breaches. In contrast, transfers from Data Processors to Data Controllers only require the Data Processor to notify and assist the Data Controller.
Onward transfers.	Article 3, Item 7.	Module One, Clause 8.7. Module Two, Clause 8.8. Module Three, Clause 8.8.	There are transparency requirements for onward transfers under the PRC and EU SCCs. See above for more details. To make an onward transfer under the PRC SCCs, the following conditions must exist: (i) the transfer is necessary, though what that entails precisely is unclear at this time; (ii) the transfer is disclosed to Subjects and, if necessary, with their consent; (iii) the transfer must be subject to a written agreement that provides protection not lower than the standards in PRC law and the assumption of joint and several liabilities for harm to Subject; and (iv) a copy of the onward transfer agreement must be provided to the Personal Information Processor. Under the EU SCCs, onward transfers much be subject to the EU SCCs or to "*a country benefitting from an adequacy decision*", a third party that ensures appropriate safeguards. The transfer is necessary for litigation purposes, or the transfer is required to protect the vital interests of others.
Entrusted Processing & Data Processors.	Article 3, Item 8.	Modules Two, Three and Four.	This is a significant area of divergence as the PRC SCCs does not significantly distinguish between types of entity that process personal information, while the EU SCCs treat Data Controllers and Data Processors very differently depending on the cross-border data transfer scenario.
Sub-processors.	Article 3, Item 8. Appendix 1.	Clause 9. Annex III.	Both SCCs seem to allow for sub-processing. However, the PRC SCCs do not explicitly address this particular issue, which means that sub-processing would be treated like any other onward transfer. As for the EU SCCs, they require sub-processors to be bound by "*in substance, the same data protection obligations as those binding the data importer*" and allow for (i) specific prior authorisation or (ii) general authorisation from a list.
Automated decision-making.	Article 3, Item 9.	Clause 10.	Under the PRC SCCs, automated decision-making must be transparent, fair, and equitable. It may not be used to apply unreasonable differential treatment in terms of transaction conditions. Under the EU SCCs, automated decision-making that produces effects concerning a subject or significantly affecting them may not occur unless the Subject consents to

			such processing or it is permitted under laws with appropriate safeguards.
Choice of law and jurisdiction.	Article 6, Items 2-5. Article 9, Item 2. Article 9, Item 5. Article 9, Item 6.	Clause 11. Clause 17. Clause 18.	The EU SCCs stipulate the law of an EU member state or, for Data Processor to Data Controller Arrangements, the laws for a country that allows for third-party beneficiary rights. It gives jurisdiction to the courts of an EU member, including the place where a Subject habitually resides. The PRC SCCs stipulate Chinese law. If a Subject, as a third-party beneficiary to the contract, brings an action, they must comply with the Civil Procedure Law of the People's Republic of China to determine jurisdiction, meaning a Chinese court with jurisdiction will be selected. In the case of the contracting parties, the contract allows for dispute resolution in a Chinese court with jurisdiction or an arbitral institution in a country that is a member of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards.
Termination and suspension.	Article 7.	Clause 16.	Under the EU SCCs, if the Data Importer breaches its obligations, the Data Exporter may suspend the contract until the breach is remedied or the contract is terminated. Several types of breaches or circumstances may trigger termination. Under the PRC SCCs, Overseas Recipients have similar rights to Data Exporters under the EU SCCs, while Personal Information Processors enjoy 2 additional grounds: (i) breach by the Overseas Recipient of the laws in the country where it is based; (ii) bankruptcy, dissolution or liquidation. Additionally, termination may also occur at the election of either party if a Regulator has issued a decision that makes execution of the contract impossible or if both parties agree to the termination.
Liability for breach of contract.	Article 8	Clause 12.	Under the PRC SCCs, "*Liability between the parties is limited to the damages suffered by the non-breaching party.*" At face value, this appears to exclude liability for lost profits. Under both SCCs, Subjects are entitled to claim damages as third-party beneficiaries. Where more than one party causes a breach of Subject rights, both are jointly and severally liable to the Subject.
Precedence.	Article 9, Item 1.	Clause 5.	Both SCCs claim to have precedence in the event of a conflict. This could cause difficulties in the event of a dispute involving both the EU and PRC.
Docking clause.	-	Clause 7.	No such mechanism exists under the PRC SCCs, which appear to be drafted for a scenario involving 2 contracting parties. Such a mechanism would be desirable for more complex processing scenarios.
Other matters agreed by the parties.	Appendix 2	-	The PRC SCCs contain a blank page at their rear. This suggests that the CAC expects contracting parties to have additional needs. However, based on current cross-border

			data transfer practices, we suspect the PRC SCCs will function as an appendix or annex rather than the main agreement.

Implications

The PRC SCCs bear some similarities with the EU SCCs but differ on some key points. Multinationals with operations in the PRC and EU that wish to rely on SCCs may need to find ways to deal with those differences and conflicts or find alternative legal paths for their cross-border data transfers.

The likely alternative for many multinationals would be to obtain "*certification of personal information protection*" that has been "*given by a professional institution in accordance with the regulations of the national cyberspace authority*" under Article 39 of the PIPL. The National Technical Committee on Information Security of Standardization Administration (also known as “TC260”) has recently issued guidance on achieving such certification but more clarity is needed on things such as who are those “professional certification institutions” and how to start the certification journey.

Finally, for those who are able to use the PRC SCCs, we have observed that many multinationals annex the EU SCCs to their own customised global data transfer agreements, and we suspect the same will happen to the PRC SCCs in time.

Will China's New Certification Rules Be a Popular Legal Path for Outbound Data Transfers?

Background

On 1 November 2021, the Personal Information Protection Law of the People's Republic of China ("**PIPL**") took effect and became the first Chinese law dedicated to protecting the personal information rights of individuals. However, due to a lack of implementation regulations and clarity, many companies face a situation where they are unsure how to comply with the PIPL in some areas.

Nowhere is this more of an issue than with Article 38 of the PIPL, which provides several conditions (or legal paths) that must be met before a cross-border data transfer may occur. According to Article 38, entities may send personal data to foreign recipients by taking one of the following legal paths:

> ***Legal Path 1 – Government Security Assessment:*** *A security assessment organised by the national cyberspace authority has been passed by the entity in accordance with Article 40 of this Law;*
>
> ***Legal Path 2 – Standard Contract:*** *A contract in compliance with the standard contract provided by the national cyberspace authority has been concluded with the overseas recipient, establishing the rights and obligations of both parties.*
>
> ***Legal Path 3 – Certification:*** *the entity has acquired a certification of personal information protection by a professional certification institution in accordance with the regulations of the national cyberspace authority; and*

On Legal Path 1 (**Government Security Assessment**), please see "*China Issues Cross-border Data Transfer Security Assessment Rules.*" For Legal Path 2 (**Standard Contract**), please see "*China Releases Draft Standard Contract for Cross-border Data transfers*" and "*Cross-border data transfers: A Comparison of the EU and Chinese Standard Contractual Clauses.*"

This article discusses China's new rules on Legal Path 3 (**Certification**).

TC260 Issues Rules for Legal Path 3 (Certification)

On 24 June 2022, the National Information Security Standardization Technical Committee (also known as "**TC260**") issued its "*Technical Specifications for the Certification of Cross-Border Processing of Personal Information*" ("**Specifications**"). The Specifications state the criteria that MNCs or other economic or business entities and overseas processors should meet to obtain certification as described in Article 38 of the PIPL (i.e., Legal Path 3). At a high level, TC260's Specifications seem to describe something like the Binding Corporate Rules ("**BCRs**") under the GDPR.

Please note that the Specifications are not compulsory. In other words, parties to cross-border personal information transfers can decide if they want to go through this Legal Path 3 and obtain certification or go through other Legal Paths as they think appropriate to legitimatise their cross-border data transfers. However, if they choose to put themselves under this certification regime, the rules under the Specifications are binding on them and relevant certification institutions.

Applicability of the Specifications

The Specifications describe certification scenarios, certification applicants and those who should bear responsibility for cross-border personal information transfers. Within an MNC, one of its entities in China can apply for certification and undertake to assume legal responsibility for the MNC's global organisation, while for an overseas entity having a not substantial presence in China, its specialised agency or designated representative in China can apply for certification and undertake to bear legal responsibility for the overseas entity.

Legally Binding Documents

Parties to cross-border personal information processing activities must sign legally binding and enforceable documents ("**LBDs**") to ensure that the rights and interests of individuals are fully protected. At a minimum, LBDs should contain:

1. The relevant parties involved in cross-border personal information processing;
2. The purpose of cross-border personal information processing and the types and scope of personal information;
3. Measures to protect the rights and interests of individuals;
4. Undertakings by each party to comply with uniform personal information processing rules and ensure that the level of personal information protection is not lower than the standards stipulated by relevant Chinese laws and regulations on the protection of personal information;
5. Undertakings to accept the supervision of certification bodies;
6. Provisions stating that relevant Chinese laws and regulations on the protection of personal information govern the arrangements;
7. Details of the organisational bodies that will bear legal responsibility within China; and
8. Provisions for compliance with other legal and regulatory obligations.

Uniform Processing Rules

Uniform processing rules, described in 4. above, must contain:

- The particulars of cross-border personal information processing, including the type, sensitivity, quantity, etc., of personal information;
- The purpose, method, and scope of cross-border personal information processing;
- The start and end time of overseas storage of personal information and the processing method after expiration;
- Transit countries involved in cross-border personal information processing;
- Resources and measures required to protect the rights and interests of individuals; and
- Rules for compensation and disposal of personal information security incidents.

DPO

Both the data exporter and foreign data importer must appoint a person to take charge of personal information protection. The persons in charge must have relevant knowledge and experience and be a part of the decision-making level of their entity. Their duties include:

- Clarifying organisational personal information protection objectives, basic requirements, work tasks, and protection measures;
- Ensuring the availability of human resources, financial support and materials for personal information protection within the organisation;
- Guiding and supporting relevant personnel in carrying out the organisation's personal information protection efforts and ensuring that personal information protection efforts achieve the expected goals; and
- Reporting to the organisation's leaders on personal information protection and promoting the continuous improvement of personal information protection efforts.

Personal Information Protection Organisation

Both the data exporter and foreign data importer should set up personal information protection internal organisations that are tasked with preventing "*unauthorised access and leakage, falsification and loss of personal information*" and undertaking the following duties:

- Formulating and implementing plans for cross-border personal information processing;
- Organising and carrying out personal information protection impact assessments ("**PIPIAs**");
- Supervising cross-border personal information transfers under rules agreed to by the relevant parties; and
- Accepting and handling requests and complaints from data subjects.

Personal Information Protection Impact Assessments (PIPIAs)

Specification is provided on what a PIPIA should contain in cross-border transfer scenarios. In particular, a PIPIA must cover:

1. Whether the provision of personal information to overseas countries complies with laws and administrative regulations;
2. The impact on the rights and interests of individuals;
3. The impact of the legal environment and network security environment of overseas countries and regions on the rights and interests of individuals;
4. Other matters necessary to safeguard the rights and interests of personal information.

Items 2. and 4. above mirror the requirements of the PIPL, while Items 1. and 3. are more specific to cross-border transfer impact assessments and suggest the need for specialised country-by-country transfer impact assessments similar to those used for GDPR purposes. For Item 3., we note that the precise meanings of "*legal environment*" and "*network security environment*" are currently unclear.

Individual Rights

Individuals have various rights over their personal information under the PIPL. Those rights include a right to access, right to correct, right to complete, right to erasure, right of portability and right to refuse processing. In addition to those rights, the Specifications provide that individuals are beneficiaries of LBDs and have the right to request a copy of the relevant LBD provisions relating to individuals' legal rights and interests.

Being a beneficiary to LBDs might, theoretically, increase the range of rights available to individuals over and above those found in the PIPL. This is especially so if MNCs operating in multiple jurisdictions take a unified highest standard approach to personal information protection at a global level.

The right to access relevant LBD provisions raises issues from a confidentiality perspective. Thus, it would be wise to stipulate such matters in a standalone document to ensure that disclosures to individuals remain appropriate.

The Specifications also provide that individuals should be allowed to litigate in the Chinese courts of their habitual place of residence against the parties to the cross-border data transfers.

Obligations of the Parties to Cross-Border Data Transfers

The provisions within the Specifications on processor obligations generally reflect the terms of the PIPL. However, further requirements are imposed on parties to cross-border data transfers, including:

- When situations arise where it is difficult to ensure the security of personal information transferred across borders, such processing must be "*promptly terminated*".
- The responsible party in China should compensate individuals for breaches arising in the context of cross-border data processing activities.

- The parties to cross-border data transfer activities should undertake to follow Chinese data protection laws, accept their application and enforcement, and cooperate with Chinese regulators' enforcement activities, such as answering their inquiries and accepting routine inspections.

Conclusions

The Specifications make Legal Path 3 (Certification) of Article 38 of the PIPL possible – though not fully actionable as China has not published a list of certification institutions to handle certification applications from entities. Nevertheless, the Specifications have provided a skeleton of the certification regime for cross-border data transfers. We believe that the Chinese authorities may issue regulations, and TC260 may also issue further guidance to substantiate this certification regime.

It should be noted that, while an entity can choose between Legal Path 3 (Certification) and Legal Path 2 (Standard Contract) to legitimatise its cross-border data transfers, Legal Path 1 (Government Security Assessment) is not optional – as long as statutory triggers exist, an entity will have to participate in a Security Assessment by the CAC (For more information see *"China Issues Cross-border Data Transfer Security Assessment Rules"*).

At this stage, it is difficult to forecast if Legal Path 3 (Certification) would be more popular than Legal Path 2 (Standard Contract). In addition to signing a cross-border data transfer contract, the Specifications essentially require that both the data exporter and the overseas data recipients are subject to a set of unified data protection rules which are aligned with Chinese laws and subject to Chinese regulators' supervision. We believe the compliance efforts would be more costly than "simply" signing the Standard Contract. However, it is possible that this certification path might be welcomed by some companies who see certification as a type of status or quality mark to signal to consumers that their personal information will be protected to higher standards.

As cross-border data transfers are a rapidly developing area of law, MNCs and overseas processors processing the personal information of people in China are advised to monitor developments in this area closely.

Our Technology, Data Protection and Cybersecurity Practice

AnJie Broad is one of the leading Chinese law firms for Technology, Data Protection and Cybersecurity matters. All leading international and Chinese legal directories have recognized our abilities.

With rich experience advising MNCs and local Chinese companies on e-commerce, telecommunications, IT, data privacy and cybersecurity issues, we are well-positioned to assist clients in managing this increasingly important risk area. We adopt a systematic approach when handling complex issues in this area and provide practical step-by-step guidance to our clients so that they can protect themselves against the risks of breaches and the consequences of failing to satisfy legal compliance requirements.

We provide full services in areas that include but are not limited to:

- Data and privacy compliance program
- Data protection officer outsourcing
- Dispute resolution
- Privacy policy
- Cross-border data transfer
- Data protection clauses
- Employee data processing
- Telecom/IT/Internet
- Hardware, software and technology
- Connected car and auto driving
- Big data and cloud services
- Important data processing
- Security incident response
- Business secret protection
- Network product certification
- Encryption
- Cybercrimes
- Lobbying and government liaison

AnJie Broad
安杰世泽