Anjie Broad
安杰世泽

Technology, Data Protection & Cybersecurity

Special Edition Newsletter

All you need to know about the Chinese Standard Contract Clauses

March 2023

Introduction

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,

On 24 February 2023, the Cyberspace Administration of China ("**CAC**") promulgated the Measures for the Standard Contract for the Export of Personal Information ("**Measures**"), which come into force on 1 June 2023, to which the Personal Information Export Standard Contract ("**Chinese SCCs**") was attached.

This Special Edition Newsletter will provide readers with an overview of the Chinese SCCs. It focuses on the following:

- When and how the Chinese SCCs can be used;
- Helping readers to understand the Measures;
- Similarities and differences with the GDPR Standard Contract; and
- Important and noteworthy clauses in the Chinese SCCs.

I have also attached a copy of the Chinese SCCs for reference purposes.

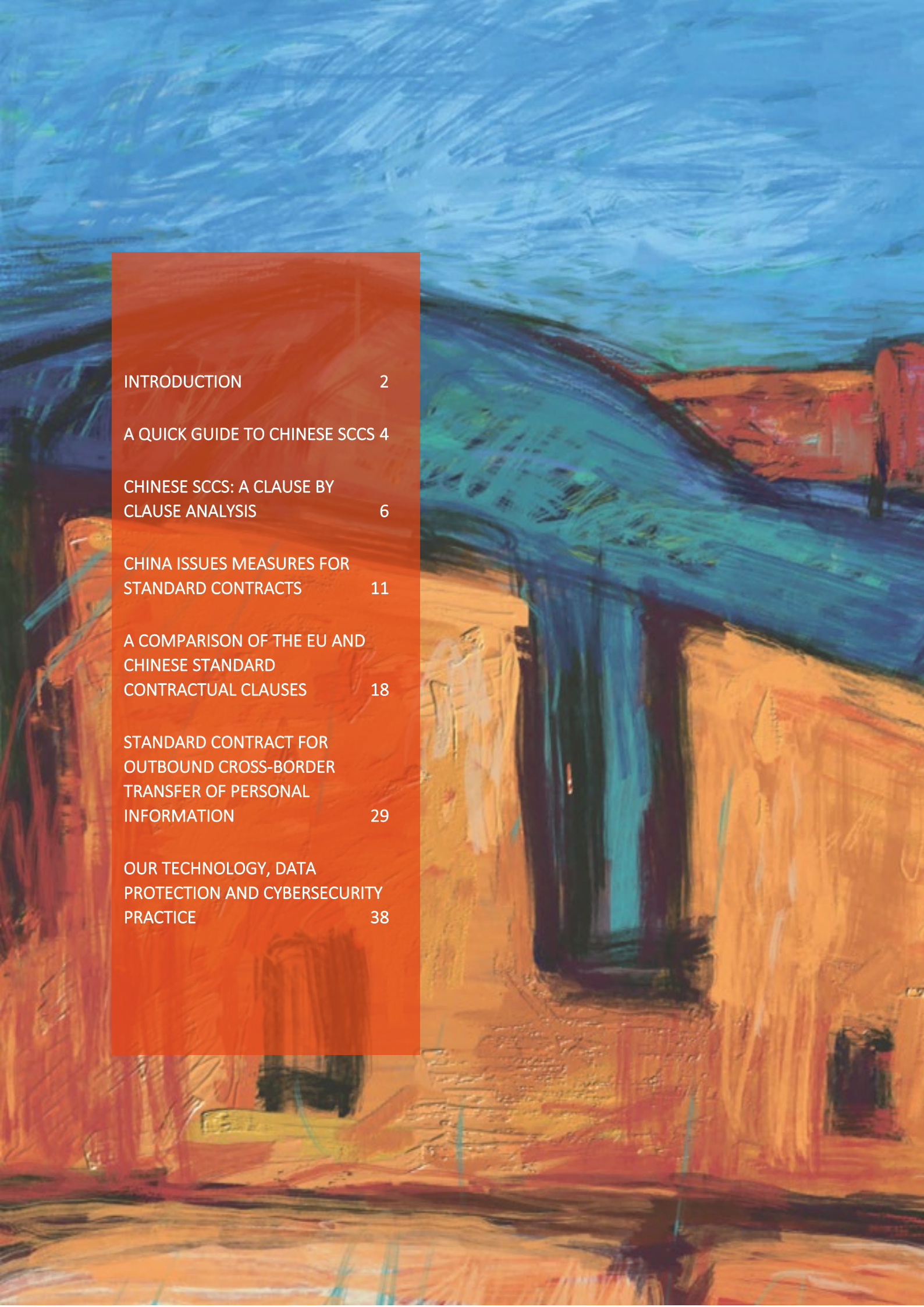
I hope that you find this Special Edition Newsletter helpful.

Please feel free to contact me if you have any questions.

Yours faithfully,

Samuel Yang

ANJIE BROAD LAW FIRM | Partner



A Quick Guide to Chinese SCCs

When can the Chinese SCCs be used?

A company can only choose to sign the Chinese SCCs, if:

- It is not a critical information infrastructure operator ("**CIIO**");
- It processes the personal information of less than one million individuals;
- It has provided personal information of less than 100,000 individuals in aggregate to overseas recipients since 1 January of the previous year; and
- It has provided sensitive personal information of less than 10,000 individuals in aggregate to any overseas recipients since 1 January of the previous year.

If any of the above conditions are not met, a company must apply to the Cyberspace Administration of China ("**CAC**") for data export security assessment, and it cannot choose to sign the Chinese SCCs.

Necessary steps to implement the Chinese SCCs

For those who can sign Chinese SCCs to legitimise their outbound data transfers, the following steps are necessary:

Outbound Data Transfer Mapping	Personal Information Protection Impact Assessment ("**PIPIA**")	Finalising the SCCs between the personal information processor and the overseas recipient	Filing the signed SCCs and the PIPIA report with the government

Step 1: Outbound Data Transfer Mapping.

This is a necessary step to understand the purpose, scope, type, quantity, sensitivity, scale and method of personal information processing by the personal information processor and the overseas recipient.

Step 2: Personal Information Protection Impact Assessment ("PIPIA").

A PIPIA is required before the personal information processor transfers personal information to any overseas recipient. A PIPIA report also needs to be filed with the government.

Step 3: Finalising the SCCs between the personal information processor and the overseas recipient.

The parties cannot change the terms of the Chinese SCCs. However, the parties will need to fill in certain information concerning intended outbound data transfers, such as: the purpose and method of processing, the scale of personal information involved, types of personal information and sensitive personal information, overseas storage period and storage location.

Step 4: Filing the signed SCCs and the PIPIA report with the government.

The signed SCCs and a completed PIPIA report need to be filed with the provincial Cyberspace Administration of China within ten (10) working days after the signed SCCs take effect.

When do companies need to complete the above steps?

The regulations governing the use of Chinese SCCs will come into force on 1 June 2023. It provides a 6-month grace period for past and current outbound data transfers. This means that companies will need to complete the above steps by 30 November 2023.

Chinese SCCs: A Clause by Clause Analysis

On 24 February 2023, the Cyberspace Administration of China ("**CAC**") promulgated the Measures for the Standard Contract for the Export of Personal Information ("**Measures**"), which come into force on 1 June 2023 ("**Effective Date**"), and to which the Personal Information Export Standard Contract ("**SCCs**") was attached.

The SCCs only apply to relevant cross-border transfers of personal information by personal information processors that have:

- not been identified as critical information infrastructure operators;
- transferred less than 100,000 individuals' personal information since 1 January in the previous year;
- transferred less than 10,000 individuals' sensitive personal information since 1 January in the previous year; and
- processed the personal information of less than 1 million individuals in total.

Relevant cross-border transfers of personal information initiated after the Effective Date must use the SCCs, while the parties to relevant cross-border transfers initiated before the Effective Date will have a six-month grace period to make new arrangements involving the SCCs. Under the Measures, the SCCs must be strictly adhered to and registered with the authorities within ten working days of signing.

Overview

The SCCs contain only nine articles and two appendices that cover all data export scenarios due to their focus on exporters and recipients rather than different processing relationships. In Chinese, the SCCs (and their appendices) contain only 18 pages (with multiple line spacing and size 14 font), which is much more condensed than its EU counterpart, i.e. the SCCs under the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**").

Article 1 - Definitions

Article 1 contains eight key definitions, namely:

- personal information processor;
- overseas recipient;
- party and parties;
- personal information subject;
- personal information;
- sensitive personal information;
- Chinese regulators; and
- relevant laws and regulations.

The meanings of undefined terms are expressly stated to be *'consistent with the meanings stipulated in the relevant laws and regulations'*.

Article 2 - Obligations of personal information processors

The obligations of personal information processors are provided in Article 2 and consist of the following:

- exporting only the necessary amount of data and doing so in accordance with the law;
- informing the personal information subject of the particulars of the overseas recipient and the processing that will occur overseas (subject to exceptions);
- ensuring that appropriate consent is in place where consent is the legal basis of processing - where minors under 14 are involved, consent should be obtained from their parents or guardians;
- recognising that the personal information subject has rights as a third-party beneficiary under the SCCs;
- ensuring that the foreign recipient will take certain technical and management measures to protect the personal information;
- providing the foreign recipient with copies of Chinese legal provisions and technical standards, whereby it is unclear if this would include a requirement to provide translations;
- responding to Chinese regulators' inquiries about overseas recipient's processing activities;
- conducting a personal information protection impact assessment in relation to the export of personal information, including the risks that the personal information will be exposed to from the general, cybersecurity, and legal environment of the country where the overseas recipient is based;
- providing a copy of the executed SCCs to a personal information subject upon request; and
- providing Chinese regulators with information, including the results of all compliance audits.

Article 3 - Obligations of overseas recipients

The obligations of overseas recipients are provided in Article 3. It is worth noting that several items in this article differentiate between the roles of the overseas recipients, i.e. as an independent personal information processor or as an entrusted processor, and stipulate different legal obligations for each role, including:

- not processing personal information beyond any consent given or the scope agreed in the SCCs;
- providing a copy of the executed SCCs to a personal information subject upon request;
- processing personal information in a way that has the least impact on personal rights and interests;
- conforming to relevant retention periods and deleting personal information if any relevant contract of entrusted processing is not in effect, invalid, revoked, or terminated; where

information is technically difficult to delete, all such processing must stop except for storage and necessary safety precautions;

- implementing technical and management measures, along with imposing confidentiality obligations and access controls on authorised personnel to ensure the security of personal information;
- taking remedial measures, notifying the personal information processor, notifying personal information subjects (when required), reporting data breaches to Chinese regulators, and documenting all circumstances related to data breaches;
- only making onward transfers outside of China when certain conditions exist, including a genuine business need, the personal information subject having been informed of the transfer (subject to exceptions), ensuring that appropriate consent is in place where consent is the legal basis of processing, imposing certain contractual conditions on onward recipients, assuming liability for the personal information rights infringement of onward recipients, providing copies of agreements with onward recipients to the personal information processor, obtaining consent from the personal information processor for sub-processing, and supervising such sub-processors;
- ensuring that automated decision-making is transparent, just, and fair;
- providing evidence of compliance and allowing audits;
- keeping objective records of processing, retaining such records for more than three years, and providing such records to Chinese regulators when legally required; and
- accepting the supervision and management of Chinese regulators, including cooperation with enquiries, inspections, and decisions.

Article 4 - The impact of policies and regulations on the protection of personal information in the country or region of the overseas recipient on the performance of the contract

Article 4 requires the parties to work together to conduct due diligence on the likely impact of the personal information destination on the performance of the contract. Some might consider such an exercise to be a transfer impact assessment covering several factors related to the personal information, the overseas data recipient, and the personal information destination.

Article 4 also provides that, where changes occur in the policies and regulations of the overseas recipient's country or region, or the government or judicial authorities of the country or region seek access to the personal information, notice must be given to the personal information processor immediately.

Article 5 - Rights of the personal information subject

All personal information subject rights recognised by the law are listed in Article 5. However, the personal information subject may also request assistance from the personal information processor or the overseas recipient to realise their rights against the overseas recipient. Where overseas recipients refuse to comply with requests from personal information subjects, they should provide reasons.

The specific third-party beneficiary rights of personal information subjects are also expressly stated in this section. Generally, only rights that the personal information processor and the overseas recipient would typically exercise against one another are excluded here.

Article 6 - Relief

Article 6 requires the overseas recipient to specify a contact person for inquiries and complaints and to provide such information concisely and easily through a separate notice or on its website.

The parties are expected to communicate and cooperate to resolve any disputes with the personal information subject. Where disputes cannot be resolved amicably, the overseas recipient is expected to accept the right of the personal information subject to complain to the Chinese regulator and file a lawsuit. The personal information subject may elect the *'relevant laws and regulations of the People's Republic of China if her or she so chooses'*.

Article 7 - Cancellation of contract

If the overseas recipient violates its obligations under the SCCs, or if there are changes in the personal information protection policies and regulations of the overseas recipient's country or region, resulting in the overseas recipient's inability to perform its obligations, the personal information processor may suspend the provision of personal information to the overseas recipient until the violation is corrected.

The personal information processor may suspend the contract and notify the Chinese regulators where:

- a suspension of personal information transfers lasts for more than one month;
- compliance with the SCCs would violate the laws of the overseas recipient's country or region;
- the overseas recipient is in material or persistent breach of the SCCs;
- the overseas recipient breaches the SCCs according to the final decision of a competent court or regulator of jurisdiction over the foreign recipient; and
- the contract is cancelled by mutual consent.

The overseas recipient must delete or return all personal information processed under the SCCs unless this is difficult to achieve, in which case processing should cease except for storage, and necessary safety measures should be taken.

Article 8 - Liability for breach of contract

The parties are liable to one another for any harm resulting from a breach of contract. The personal information subject can request either or both parties to assume liability for violating the personal information subject's rights. Where a party assumes more than its share of liability, it can seek to recover from the other party.

Article 9 - Other

Article 9 provides that the SCCs are to prevail in a conflict with any other legal document entered by the parties. It is unclear how such provisions would interact with the standard contracts of other

jurisdictions. It also states that Chinese law applies to the formation, validity, performance, and interpretation of the SCCs, and any dispute related to the SCCs between the parties.

Boilerplate provisions for notices under the SCCs are included. They require the inclusion of contact details by the parties.

The jurisdiction clause within Article 9 is interesting because it gives the parties the option to select a forum for resolving disputes, which includes arbitral tribunals outside of China in countries that are parties to the New York Convention. How this will work in practice remains to be seen.

An interpretation clause provides that the SCCs must be interpreted in accordance with laws and regulations, and not in any way that contradicts the rights and obligations under such laws and regulations. This could perhaps be regarded as a purposive approach to contractual interpretation.

Appendix 1

This contains the details of the personal information export, including the purpose and methods of processing, the scale of personal information, the types of personal information as classified by the Information Security Technology - Personal Information Security Specification (GB/T 35273-2020), permitted onward recipients, mode of transmission, retention period, overseas storage location, and other matters.

Appendix 2

This is reserved for *'Other matters agreed by the parties'*.

Conclusions

Companies engaged in relevant cross-border data transfers will need to incorporate the SCCs into their data transfer arrangements. We advise companies to tackle the adoption of the SCCs early on to avoid problems later, such as overseas recipients refusing to use the SCCs. Such issues could cause business disruption for some companies if they unsuccessfully try to address them towards the end of the grace period.

China Issues Measures for Standard Contracts

On 22 February 2023, the Cyberspace Administration of China ("**CAC**") promulgated the Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information ("**Measures**"), which come into force on 1 June 2023 ("**Effective Date**"). This article reproduces the content of the Measures in English and provides an analysis based on the wording of the text, our observations, and statements by the CAC.

Article 1

Text

"The Measures are formulated in accordance with the Personal Information Protection Law of the People's Republic of China and other laws and regulations to protect personal information rights and interests and regulate the outbound cross-border transfer of personal information."

Analysis

While the Measures are formulated per the Personal Information Protection Law ("**PIPL**"), other laws and regulations influence how the Measures should be understood and interpreted.

Article one of the Standard Contract defines relevant laws and regulations as follows:

*"**Relevant laws and regulations** refer to the laws and regulations of the People's Republic of China, such as the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, the Civil Code of the People's Republic of China, the Civil Procedure Law of the People's Republic of China, and the Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information."*

Therefore, it would be safe to assume that relevant laws and regulations include, at least, the abovementioned laws and regulations.

Article 2

Text

*"The Measures apply to the provision of personal information to any recipient outside of the territory of the People's Republic of China by a personal information processor under a standard contract for outbound cross-border transfer of personal information executed with such overseas recipient (hereinafter referred to as the "**Standard Contract**")."*

Analysis

Regarding the entities subject to the Measures, some might note the use of the term personal information ("**PI**") processor. A PI processor, as defined in Article 73 of the PIPL, is an entity that independently determines the purpose and method of processing in their PI processing activities. In contrast, an entrusted processor, as defined in the context of Article 21 of the PIPL, processes personal information based on the instructions of a PI processor.

We have observed in practice that business arrangements can be more complex than a transfer from A to B. Some might involve transfers from (i) a Chinese PI processor to (ii) a Chinese entrusted

processor to (iii) an overseas recipient. In such a scenario, the parties in China may disagree over who should sign the Standard Contract with the overseas recipient.

We believe that the Chinese PI processor should bear the obligation of signing a Standard Contract with an overseas recipient to enable the Chinese entrusted processor to export such data to that overseas recipient. Our reasoning is that entrusted processors can only act on the instructions of a PI processor. Therefore, if the entrusted processor makes a transfer to an overseas recipient under the instructions of a PI processor, such actions are attributable to the PI processor. However, in the above example, we believe that if the PI processor fails to sign a Standard Contract with the overseas recipient, it would be prudent for the entrusted processor to sign a Standard Contract with the overseas recipient.

As for overseas recipients, their key defining characteristics are that they are overseas and receive PI from China, regardless of whether they are PI processors, entrusted processors or sub-processors.

Article 3

Text

"Where personal information is transferred overseas under a Standard Contract, a practice of independent contracting combined with compliance with the record-filing requirement, and protection of rights combined with prevention of risks shall be maintained to ensure a secure and free flow of personal information across borders."

Analysis

Article 3 is very high-level in nature and adds little to the requirements of pre-existing laws and regulations, except for the record-filing requirement, on which we will comment below.

Article 4

Text

"To provide personal information to an overseas recipient under a Standard Contract executed, a personal information processor shall meet the following criteria:
(1) not a critical information infrastructure operator;
(2) handling personal information of less than one million individuals;
(3) having provided personal information of less than 100,000 individuals in aggregate to overseas recipients since 1 January of the previous year; and
(4) having provided sensitive personal information of less than 10,000 individuals in aggregate to any overseas recipients since 1 January of the previous year.
Where it is otherwise provided in any law or administrative regulations, or by the national cyberspace authority, those provisions shall prevail.
A personal information processor must not split up the amount of the personal information to be transferred overseas or adopt other means to provide to any overseas recipient under a Standard Contract such personal information whose outbound cross-border transfer should be subject to a security assessment according to law."

Analysis

The eligibility criteria for Standard Contracts mirror and complement those found in the Measures for the Security Assessment of Outbound Data Transfers. In other words, PI processors may only sign the Standard Contracts when they are not under a legal obligation to go through a cross-border data

transfer security assessment by the CAC ("**Security Assessment**"). However, it is interesting that what can perhaps be described as a non-abuse provision has been added to the second paragraph compared with the Draft Provisions for the Standard Contract for Outbound Cross-border Transfer of Personal Information ("**Draft Provisions**") previously issued by the CAC. This is especially noteworthy for MNCs that have many China subsidiaries transferring PI overseas separately. To avoid regulatory suspicion of abuse, we suggest that MNCs carefully examine the aggregated amount of PI transferred by their subsidiaries to understand their overall situation fully and decide if the Security Assessment would apply instead.

How this non-abuse provision will be enforced in practice raises many questions. However, it does suggest that the CAC may eventually claim the power to exercise significant discretion over such matters.

Article 5

Text

"Before providing any personal information to an overseas recipient, a personal information processor shall conduct a personal information protection impact assessment focused on the following matters:
(1) the legality, legitimacy, and necessity of the purpose, scope, and method of the personal information processing by the personal information processor and the overseas recipient;
(2) the quantity, scope, type, and sensitivity of personal information to be transferred overseas, and the risk that the outbound cross-border transfer may pose to personal information rights and interests;
(3) the responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management and technical measures and capabilities of the overseas recipient to perform such responsibilities and obligations are sufficient to ensure the security of personal information to be transferred;
(4) the risk of the personal information being tampered with, sabotaged, disclosed, lost, or misused after it is transferred overseas, and whether there is a smooth channel for individuals to protect their personal information rights and interests;
(5) the impact of personal information protection policies and regulations in the country or region where the overseas recipient is located on the performance of the Standard Contract; and
(6) other matters that may affect the security of personal information to be transferred overseas."

Analysis

Article 5 prescribes certain things that must be assessed within a personal information impact assessment ("**PIPIA**") before an outbound transfer of PI is made (as opposed to before signing the Standard Contract).

Matter (3) will require PI processors to have certain technical capabilities to assess whether an overseas recipient is, in fact, capable of performing relevant management and technical measures. This may require smaller companies and start-ups lacking such expertise to outsource the performance of those parts of the PIPIA, which will increase the costs associated with making outbound transfers.

Matter (4) will require PI processors to have a certain degree of knowledge about the PI destination. For some countries and regions, this will be a very straightforward exercise. However, for others, particularly where language barriers exist, PI processors will either need to rely on overseas

recipients or seek the assistance of suitably qualified experts, such as legal professionals or information security experts.

Matter (5) essentially requires an analysis of the PI destination. This may require the involvement of foreign legal counsel to ensure that a fair and accurate PIPIA is generated.

Article 6

Text

"A Standard Contract shall be executed in strict accordance with the content of the annex of the Measures. The national cyberspace authority may adjust the content of the annex based on the actual situation.
A personal information processor may agree on other terms with an overseas recipient, provided that such terms must not conflict with the terms of the Standard Contract.
An outbound cross-border transfer of personal information can be carried out only after the Standard Contract for such transfer takes effect."

Analysis

A conservative reading of Article 6 might lead to the conclusion that the Standard Contract (the annex of the Measures) should not be modified (except for its placeholders) in any way whatsoever. In practice, we expect the Standard Contract to be treated as an annex to a customised data transfer agreement ("**DTA**"), in much the same way as is done with the SCCs under GDPR, to avoid modification and provide the parties with the maximum degree of flexibility permissible. Such customised DTA's will likely contain ranking clauses which provide that the Standard Contract will prevail in a conflict between the Standard Contract and the customised DTA.

The Measures make it clear that the Standard Contract must be effective before PI transfers begin. As such, PI processors will need to ensure that internal controls exist to ensure compliance.

Article 7

Text

"A personal information processor shall, within 10 working days from the effective date of a Standard Contract executed, file a record with the provincial cyberspace authority where it is domiciled by submitting the following materials:
(1) the Standard Contract; and
(2) a personal information protection impact assessment report.
The personal information processor shall be responsible for the authenticity of the materials submitted."

Analysis

While it is clear that Standard Contracts must be registered along with a PIPIA report, the registration process remains unclear. We expect guidelines to be announced before the Measures become effective.

Based on informatisation trends in China, the CAC may establish an online filing system to facilitate filings.

Article 8

Text

"If any of the following circumstances occurs during the validity term of a Standard Contract, the personal information processor shall conduct a personal information protection impact assessment again, and supplement the existing Standard Contract or execute a new Standard Contract, as well as file a record again:
(1) there is any change in the purpose, scope, type, sensitivity, quantity, method, retention period, and storage location of the personal information transferred overseas, or any change in the purpose and method of the personal information processing of the overseas recipient, or an extension of the overseas retention period of the personal information;
(2) there is any change in personal information protection policies and regulations in the country or region where the overseas recipient is located, which may affect personal information rights and interests; or
(3) other circumstances that may affect personal information rights and interests."

Analysis

The main takeaway from Article 8 is that the circumstances related to a Standard Contract need to be monitored. If any changes occur, a fresh PIPIA will be required.

Article 8 mentions that an existing standard contract may need to be supplemented or a new Standard Contract may need to be executed, "*as well as file a record again*". From the context, it appears that a supplement to an existing Standard Contract also needs to be filed.

We note that circumstance (2) might prove particularly onerous for some businesses, given that legal developments will need to be monitored in all PI destinations. This particular obligation will probably increase the costs of cross-border data transfers for some PI processors.

Article 9

Text

"Cyberspace authorities and their staff members shall keep confidential any personal privacy, personal information, trade secrets, or confidential business information that they come to know in the course of the performance of their duties, and must not disclose or illegally provide to others or use such information."

Analysis

Other laws and regulations contain similar restrictions. Though not explicitly stated in the Measures, we note that CAC staff members face potential civil and criminal liabilities for violating Article 9.

Article 10

Text

"Any organisation or individual who finds that a personal information processor provided personal information to any overseas recipient in violation of the Measures may report the case to a cyberspace authority at or above the provincial level."

Analysis

It is unclear how individuals will discover if their information is transferred to an overseas recipient in practice. However, this is good for PI subjects in the sense that there is a clear indication of where they can direct their reports.

Article 11

Text

"Where a cyberspace authority at or above the provincial level finds any considerable risk or any personal information security incident in relation to an activity of outbound cross-border transfer of personal information, it may conduct a regulatory talk with the personal information processor concerned according to law. The personal information processor shall rectify and eliminate the risk as required."

Analysis

The content of Article 11 begs the question: How will the authorities find "*any considerable risk"*? One obvious answer might involve reports from members of the public (under Article 10) and disgruntled employees. However, it is also possible that a system of spot checks in accordance with Article 64 of the PIPL could be implemented to ensure that PI processors take their obligations seriously.

On the other hand, compared with the previous Draft Provisions, which stipulate that a cyberspace authority at or above the provincial level shall *"notify in writing to … immediately terminate the outbound cross-border transfer"* in the case of non-compliance, the Measures take a softer approach. They seem to allow PI processors to rectify and eliminate risks without explicitly requiring them to cease overseas transfers of PI.

Article 12

Text

"Anyone who violated the Measures shall be dealt with in accordance with the Personal Information Protection Law of the People's Republic of China and other laws and regulations; and there shall be investigation for criminal liability according to law if the violation constitutes a criminal offense."

Analysis

As punishments for violating the Measures can be based on the PIPL, it seems that penalties for violations of the Measures can be as high as 5% of a PI processor's annual revenue, the confiscation of illegal income, the cancellation of business licenses, and the penalisation of individuals directly responsible. Criminal liability may apply in addition to the foregoing.

Article 13

Text

"The Measures shall come into force on 1 June 2023. Any activity of outbound cross-border transfer of personal information initiated before the entry into force of the Measures that does not comply with the Measures shall be rectified within 6 months from the date of entry into force of the Measures."

Analysis

For transfers started before 1 June 2023, PI processors have 6 months to comply with the Measures. For transfers that began on or after 1 June 2023, PI processors must comply with the Measures before initiating any transfer to overseas recipients.

Concluding thoughts

The Measures add another layer of compliance obligations for businesses to deal with. We believe that many businesses' most difficult compliance obligation will be conducting PIPIA and monitoring conditions at the PI destination. While we are inclined to believe that external service providers can meet such needs, this will add costs for businesses that need to transfer PI overseas.

Considering the nature of obligations that need to be implemented under the Measures, we believe that the early issuance of the Measures plus a 6-month grace period is sufficient for many enterprises to transition to the Standard Contract. However, to avoid unexpected events, we suggest that PI processors contact their overseas recipients as soon as possible to implement new arrangements between them that comply with the Standard Contract.

A Comparison of the EU and Chinese Standard Contractual Clauses

Background

On 24 February 2023, the Cyberspace Administration of China ("**CAC**") promulgated the Measures for the Standard Contract for the Export of Personal Information ("**Measures**"). The Measures take effect on 1 June 2023 and open a lawful path for cross-border data transfers under Article 38 of the Personal Information Protection Law ("**PIPL**").

The Measures contain a Standard Contract for Outbound Cross-border Transfer of Personal Information ("**Chinese 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 Chinese SCCs may only be used in the following relevant cross-border transfer scenarios:

(1) Transfers by non-critical information infrastructure operators;
(2) Transfers by a Personal Information Processor that has handled the personal information of fewer than 1 million people;
(3) Transfers by a Personal Information Processor that has made outbound transfers of personal information of fewer than 100,000 people since 1 January of the previous year; and

(4) Transfers by a Personal Information Processor that has made outbound transfers of sensitive personal information of fewer than 10,000 people since 1 January of the previous year.

General Observations

We note that the Chinese 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 Chinese SCCs can be considered a single document that applies to all relevant cross-border data transfers because Chinese law does not explicitly distinguish between Personal Information Processors and Entrusted Processors.

In contrast to the Chinese 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 Chinese SCCs and EU SCCs. The table matches various topics identified within each document to specific provisions.

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
Definitions and interpretation.	Article 1	Clause 1. Clause 4.	The Chinese SCCs provide 8 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 defined in the Chinese SCCs. However, the term "entrusted" is used on a handful of occasions. To express this in GDPR terms, the Chinese SCCs do not explicitly recognise the existence of Data Processors.

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
Sensitive personal information and special categories of personal data.	Article 1.	Module One, Clause 8.6.	The EU SCCs and the Chinese SCCs provide definitions. However, 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 Chinese 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 Chinese 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 Chinese 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.

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
Personal Subject or Data Subject (collectively or generally, "Subject") rights.	Article 2, Item 4. Article 2, Item 9. Article 3, Item 3. 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 Chinese 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 5.	Clause 8.	Personal Information Processors must, under the Chinese 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 5. Article 3, Item 6.	Module One, Clause 8.5. Module Two, Clause 8.6.	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.

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
		Module Three, Clause 8.6. Module Four, Clause 8.2.	Concerning access controls, there appears to be broad equivalence between the SCCs. However, the Chinese SCCs explicitly require Overseas Recipients to have "*a minimum authorised access control policy…*"
Provision of laws and technical standards.	Article 2, Item 6.	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 7. Article 3, Item 13.	Module One, Clause 8.9. Clause 13.	Under the Chinese 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 Chinese 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 Chinese 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 8. 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,

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
			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 Chinese SCCs, we expect that many such forms or templates will likely be variations of styles used in the EU. Based on the implementation of the Security Assessment Measures in practice, we believe that the CAC will expect Personal Information Processors to approach impact assessments with a high degree of granularity. Given that such assessments must be filed with the CAC, it should be very easy for them to check whether an impact assessment has been carried out in an appropriate manner.
Compliance and record keeping.	Article 2, Item 10. Article 3, Item 11-13.	Module One, Clause 8.9. Module Two, Clause 8.9. Module Three, Clause 8.9. Module Four, 8.3	Under the Chinese 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 reverse burden of proof. However, such a reverse burden of proof could exist in disputes with Subjects. Overseas Recipients under the Chinese 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.

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
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 Chinese SCCs require a clear statement on the quantity of personal information transferred and suggests using the personal information categories listed in recommended national standard GB/T35273.
Access by government authorities at destination.	Article 3, Item 9. Article 4, Item 6.	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 Chinese SCCs provisions on dealing with foreign government or judicial authorities is limited to a statement that they must be reported to the Personal Information Processor. 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 5. 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 Chinese SCCs, an Entrusted Processor who is an Overseas Recipient must provide an audit report after deletion or anonymisation.
Data breaches.	Article 3, Item 7.	Module One, Clause 8.5. Module Two, Clause 8.6.	Under the Chinese 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

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
		Module Three, Clause 8.6. Module Four, 8.2.	as insurance, have reporting requirements that can be as short as 30 minutes. 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 8.	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 Chinese SCCs, the following conditions must exist: (i) there is an actual business need, 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 must be subject to the EU SCCs, or to "*a country benefitting from an adequacy decision*", a third party that ensures appropriate safeguards, necessary for litigation purposes, or 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 Chinese SCCs do not significantly distinguish between types of entities that process personal information, while the EU SCCs treat Data

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
			Controllers and Data Processors very differently depending on the cross-border data transfer scenario.
Sub-processors.	Article 3, Item 8. Article 3, Item 9. Appendix 1.	Clause 9. Annex III.	Both SCCs seem to allow for sub-processing. We believe sub-processing under the Chinese SCCs is subject to the same rules as onward transfers. However, in addition to the onward transfer rules, it seems that sub-processing is also subject to the consent of the Personal Information Processor, that a sub-processor must adhere to the agreed purpose and method of processing agreed between the parties, and that the Overseas Recipient must supervise the sub-processor. 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 10.	Clause 10.	Under the Chinese 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 4 and 5. Article 9, Item 2. Article 9, Item 4.	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.

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
			The Chinese SCCs stipulate Chinese law. If a Subject, as a third-party beneficiary to the contract, brings an action, they may file a lawsuit in accordance with the Civil Procedure Law of the People's Republic of China to determine jurisdiction, meaning a Chinese court with jurisdiction should be selected. In the case of the contracting parties, the Chinese SCCs 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 Chinese SCCs, Overseas Recipients have similar rights to Data Exporters under the EU SCCs, while Personal Information Processors enjoy an additional ground: breach by the Overseas Recipient of the laws in the country where it is based.
Liability for breach of contract.	Article 8	Clause 12.	Under the Chinese 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 Chinese SCCs, which appear to be drafted for a scenario

Topic	Chinese SCCs	GDPR SCCs	AnJie Broad's Comments
			involving 2 contracting parties. Such a mechanism would be desirable for more complex processing scenarios.
Other matters agreed by the parties.	Appendix 2	-	The Chinese 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 Chinese SCCs will function as an appendix or annex rather than the main agreement.

Implications

The Chinese 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. However, as this Legal Path is still at its infant stage and generally lacks transparency, we believe that companies should wait for further guidance in this area before they seek certification.

Finally, for those who are able to use the Chinese 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 Chinese SCCs in time. However, we believe that such annexed Chinese SCCs must also been signed by parties as they need to be filed with the government.

Standard Contract for Outbound Cross-border Transfer of Personal Information

(English Translation)

Drafted by the Cyberspace Administration of China

In order to ensure that the activities of personal information processing by the overseas recipient meet the personal information protection standards stipulated in the relevant laws and regulations of the People's Republic of China, and to clarify the rights and obligations of the personal information processor and the overseas recipient regarding personal information protection, the parties, upon negotiation, hereby enter into this contract (the "Contract").

Personal Information Processor:

Address:

Contact Information:

Contact Person:_____Title:

Overseas Recipient:

Address:

Contact Information:

Contact Person:_____Title:

Whereas the personal information processor and the overseas recipient carry out the activities of outbound cross-border transfer of personal information in accordance with the covenants hereof, for the commercial behaviours related to these activities, the parties [have] / [have agreed] to sign a commercial contract on XX, if any, on MM/DD/YY.

The main body of the Contract is formulated in accordance with the Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information, and, without prejudice thereto, any other covenants by and between the parties may be detailed in Appendix II, which forms an integral part hereof.

Article 1 Definition

For the purpose of the Contract, except as otherwise stipulated in the context:

1. "Personal information processor" refers to any organisation or individual that independently determines the purpose and method of processing in their personal information processing activities and provides personal information to a recipient outside the territory of the People's Republic of China.

2. "Overseas recipient" refers to an organisation or individual located outside the territory of the People's Republic of China that receives personal information from the personal information processor.

3. The personal information processor or the overseas recipient shall be referred to individually as a "party", and collectively as the "parties".

4. "Personal information subject" refers to the natural person identified by or associated with the personal information.

5. "Personal information" refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymised.

6. "Sensitive personal information" refers to personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical and health condition, financial account, personal location tracking and other information of a natural person, as well as any personal information of a minor under the age of 14.

7. "Regulatory authority" refers to the cyberspace administration department of the People's Republic of China at or above the provincial level.

8. The term "relevant laws and regulations" refers to the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, the Civil Code of the People's Republic of China, the Civil Procedure Law of the People's Republic of China, the Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information, and other laws and regulations of the People's Republic of China.

9. The meanings of other undefined terms herein shall be consistent with those given in the relevant laws and regulations

Article 2 Obligations of the personal information processor

The personal information processor shall perform the following obligations:

1. The processing of any personal information shall comply with relevant laws and regulations, and the personal information provided overseas shall be limited to the minimum scope necessary for achieving the purpose of processing.

2. The personal information subject shall be informed of the name or title of the overseas recipient, its contact information, the purpose and method of processing, the category and storage period of personal information, the method and procedure for exercising the rights of the personal information subject, and other matters in Appendix I "Instructions on Outbound Cross-border Transfer of Personal Information"; if any sensitive personal information is involved, the personal information subject shall also be informed of the necessity to provide the sensitive personal information and the impact on the individual, except where relevant laws and administrative regulations stipulate that it is not required to inform the personal information subject.

3. If the personal information shall be provided overseas based on individual consent, specific consent from the personal information subject shall be obtained; if any personal information of a minor under the age of 14 is involved, the specific consent from the minor's parents or other guardians shall be obtained; if written consent is required by laws or administrative regulations, such written consent shall be obtained.

4. The personal information subject shall be informed that the personal information processor and the overseas recipient have agreed through the Contract that the personal information subject is a third-party beneficiary, and that the personal information subject may enjoy the rights of a third-party beneficiary pursuant to the Contract if he or she does not expressly refuse within 30 days.

5. Reasonable efforts shall be made to ensure that the overseas recipient will fulfil its obligations hereunder by adopting the following technical and management measures (upon fully considering the purpose of personal information processing, the type, scale, scope and sensitivity of personal information, the quantity and frequency of transmission, the period of transmission and storage of personal information by the overseas recipient, and other possible risks to the security of personal information): (Technical and management measures, such as encryption, anonymisation, de-identification, access control, etc.)

6. At the request of the overseas recipient, the personal information processor shall provide the overseas recipient with a copy of the relevant legal provisions and technical standards.

7. The personal information processor shall respond to the inquiries from the regulatory authority regarding the personal information processing activities of the overseas recipient.

8. Personal information protection impact assessment shall be conducted in accordance with relevant laws and regulations for the activities that are intended to provide personal information to the overseas recipient, which shall focus on the following contents:

(1) the legality, legitimacy, and necessity of the purpose, scope, and method for processing personal information by the personal information processor and the overseas recipient;

(2) the quantity, scope, type, and sensitivity of the personal information to be transferred overseas, and the risks that may be posed to the rights and interests in personal information by outbound cross-border transfer of personal information;

(3) the obligations that the overseas recipient undertakes to assume, and whether its management and technical measures and capabilities to fulfil such obligations are sufficient to ensure the security of personal information to be transferred overseas;

(4) the risk of being tampered with, destroyed, leaked, lost, or illegally used after the personal information is transferred overseas, and whether there is a smooth channel for individuals to protect their rights and interests in the personal information;

(5) an assessment of the possible impact of local personal information protection policies and regulations on the performance of the Contract in accordance with Article 4 hereof; and

(6) other matters that may affect the security of personal information to be transferred overseas.

The personal information protection impact assessment report shall be retained for at least three years.

9. A copy of the Contract shall be provided to the personal information subject upon request. If any trade secret or confidential business information is involved, relevant contents therein may be properly processed without affecting the understanding of the personal information subject.

10. The personal information processor shall assume the burden of proof for performance of its obligations hereunder.

11. The information referred to in Article 3.11 hereof shall be provided to the regulatory authority as required by relevant laws and regulations.

Article 3 Obligations of the overseas recipient

The overseas recipient shall perform the following obligations:

1. The overseas recipient shall process the personal information in accordance with the covenants listed in Appendix I "Instructions on Outbound Cross-border Transfer of Personal Information; if it needs to process any personal information beyond the purpose or method of processing, or the category of personal information as agreed, the specific consent from the personal information subject shall be obtained in advance; if any personal information of a minor under the age of 14 is involved, the specific consent from the minor's parents or other guardians shall be obtained.

2. If entrusted by a personal information processor to process any personal information, the overseas recipient shall process the personal information in accordance with its covenants with the personal information processor and shall not process any personal information beyond the purpose and method of processing as agreed with the personal information processor.

3. A copy of the Contract will be provided to the personal information subject upon request. If any trade secret or confidential business information is involved, relevant contents therein may be properly processed without affecting the understanding of the personal information subject.

4. The personal information shall be processed in a way that has minimum impact on the individual rights and interests.

5. The storage period for personal information shall be the minimum time necessary to achieve the purpose of processing; if the storage period expires, personal information (including all backups) shall be deleted. If entrusted by a personal information processor to process any personal information, when the entrustment contract is yet to be effective, becomes invalid, is cancelled, or terminated, the overseas recipient shall return the personal information to the personal information processor or delete it, and shall provide a written explanation to the personal information processor. If it is technically difficult to realise the deletion of the personal information, the overseas recipient shall cease any processing apart from storage and necessary security measures.

6. The overseas recipient shall ensure security in the processing of personal information by the following means:

(1) adopting effective technical and management measures including but not limited those specified in Article 2.5 hereof and carrying out regular inspection to ensure the security of personal information.

(2) ensuring that all persons authorised to process personal information will fulfil their confidentiality obligations and establishing minimum authorised access control.

7. If the processed personal information is or may be tampered with, destroyed, leaked, lost, illegally used, or provided or accessed in an unauthorised way, the overseas recipient shall carry out the following work:

(1) adopting timely and appropriate remedial measures to mitigate the adverse impact on the personal information subject;

(2) immediately notifying the personal information processor and report to the regulatory authority as required by relevant laws and regulations. The notification shall include the following matters:

a. the category of personal information subject to, the reasons for, and the possible impact of falsification, destruction, leakage, loss, illegal use, or unauthorised provision or access;

b. the remedial measures that have been adopted;

c. the measures that can be adopted by the personal information subject to mitigate the harm; and

d. the contact information of the person or team responsible for handling relevant circumstances;

(3) giving notification to the personal information subject, if required by the relevant laws and regulations, in which case the content of the preceding Item (2) shall be included in the notification (if entrusted by the personal information processor to process any personal information, the notification shall be given by the personal information processor);

(4) recording all facts related to the falsification, destruction, leakage, loss, illegal use, or unauthorised provision or access that have

occurred or may occur, including all remedial measures adopted, and retaining such records.

8. The overseas recipient shall not provide any personal information to a third party outside the territory of the People's Republic of China, unless the following conditions are met simultaneously:

a. There is an actual business need.

b. The personal information subject has been informed of the name or title of the third party, its contact information, the purpose of processing, the method of processing, the category of personal information, the storage period, the method and procedure for exercising the rights of the personal information subject, and other matters; if any sensitive personal information is provided to the third party, the personal information subject shall also be informed of the necessity to provide sensitive personal information and the impact on the individual rights and interests, except where relevant laws and administrative regulations stipulate that it is not required to inform the personal information subject.

c. If the processing of personal information is based on individual consent, the specific consent from the personal information subject shall be obtained; if the personal information of a minor under the age of 14 is involved, the consent from the minor's parents or other guardians shall be obtained; if written consent is required by laws or administrative regulations, such written consent shall be obtained.

d. It has reached a written agreement with the third party to ensure that the third party's activities of personal information processing meet the personal information protection standards stipulated in relevant laws and regulations of the People's Republic of China, and it will assume the legal liability for damaging the rights of the personal information subject due to provision of personal information to a third party outside the territory of the People's Republic of China; and

e. It will provide a copy of the aforesaid written agreement to the personal information subject upon request; if any trade secret or confidential business information is involved, relevant contents therein may be properly processed without affecting the understanding of the personal information subject.

9. If the overseas recipient is entrusted by a personal information processor to process personal information, and then subcontracts the processing to a third party, the consent from the personal information processor shall be obtained in advance, and it shall require the third party entrusted to process the personal information in accordance with the purpose and method of processing as agreed in Appendix I "Instructions on Outbound Cross-border Transfer of Personal Information" hereof, and shall supervise the personal information processing activities of such third party.

10. Where any personal information is used for automated decision making, the overseas recipient shall ensure transparency in decision making and fair and equitable results, and shall not apply unreasonable differential treatment to personal information subjects in terms of transaction price and other transaction conditions; if giving push information and commercial marketing to personal information subjects through automated decision making, it shall provide options to avoid targeting their personal characteristics or provide a convenient method for rejection.

11. The overseas recipient shall undertake that it will provide the personal information processor with all necessary information required for compliance with the obligations hereunder, allow the personal information processor to consult all necessary data files and documents, or conduct audits of the processing activities hereunder, and provide convenience for such audits conducted by the personal information processor.

12. The overseas recipient shall maintain objective records of the personal information processing activities and retain such records for at least three years; it shall provide the relevant records and documents to the regulatory authority directly or through the personal information processor as required by relevant laws and regulations.

13. The overseas recipient shall agree to accept the supervision and management by the regulatory authority in the relevant procedures for monitoring the performance of the Contract, including but not limited to responding to the regulator's inquiries, cooperating in its inspections, obeying the measures taken or decisions made by the regulatory authority, and providing written proof that necessary actions have been taken.

Article 4 Impact of personal information protection policies and regulations in the country or region where the overseas recipient is located on the performance of the Contract

1. The parties shall warrant that they have exercised reasonable care at the time of conclusion hereof and are not aware of any personal information protection polices or regulations in the country or region where the overseas recipient is located that affect the performance of its obligations hereunder (including any requirements to provide personal information or to authorise public authorities to access personal information).

2. The parties represent that, in providing the warranties in Article 4.1, assessment has been made based on the following circumstances:

(1) the specific circumstances of the outbound cross-border transfer, including the purpose of personal information processing, the category, scale, scope and sensitivity of the personal information to be transferred, the scale and frequency of transmission, the period for personal information transfer and storage by the overseas recipient, the overseas recipient's previous experience in similar outbound cross-border transfer and processing of personal information, whether the overseas recipient has encountered any personal information security incident and whether it has handled the incident in a timely and effective manner, whether the overseas recipient has received any request for personal information from a public authority in the country or region where it is located and the overseas recipient's response;

(2) the personal information protection policies and regulations of the country or region where the overseas recipient is located, including the following factors:

a. the current laws and regulations and generally applicable standards on personal information protection in such country or region;

b. the regional or global organisations on personal information protection of which such country or region is a member, and the binding international commitments it has made; and

c. the mechanism for the implementation of personal information protection in such country or region, such as whether there is any personal information protection supervision and enforcement body and relevant judicial body, etc.;

(3) the security management system of the overseas recipient and its capabilities to guarantee technical means.

3. The overseas recipient warrants that it has made its best efforts to provide the personal information processor with all necessary relevant information in the assessment under Article 4.2.

4. The parties shall document the processes and results of the assessment under Article 4.2.

5. If the overseas recipient is unable to perform the Contract due to any change in personal information protection policies and regulations of its country or region (including a change in laws or mandatory measures in such country or region), the overseas recipient shall notify the personal information processor of such change immediately after it is aware of such change.

6. The overseas recipient shall immediately notify the personal information processor after receiving a request to provide any personal information hereunder from a government authority or judicial body of the country or region where it is located.

Article 5 Rights of the personal information subject

The parties agree that the personal information subject shall have the following rights as a third-party beneficiary hereunder:

1. The personal information subject has the right to be informed, the right to make decision, the right to restrict or refuse the processing of his or her personal information by others, the right to request for accessing, copying, correcting, supplementing, and deleting his or her personal information, and the right to request an explanation of the rules for the processing of his or her personal information in accordance with relevant laws and regulations.

2. To exercise the aforesaid rights in the personal information that has been transferred overseas, the personal information subject may request the personal information processor to take appropriate measures to realise the rights, or make a request directly to the overseas recipient. If the personal information processor fails to do so, it shall notify and request the overseas recipient to assist in realising such rights.

3. The overseas recipient shall realise the legitimate rights of the personal information subject within a reasonable period, as required by the notice of the personal information processor or at the request of the personal information subject.

The overseas recipient shall truthfully, accurately, and fully disclose relevant information to the personal information subject in a prominent way and in understandable language.

4. If the overseas recipient rejects the request of the personal information subject, it shall inform the

personal information subject of the reasons for its rejection and the channels by which the personal information subject may file a complaint with the relevant regulatory authority and seek judicial remedy.

5. The personal information subject as a third-party beneficiary hereunder shall have the right to demand the performance of the following provisions regarding the rights of the personal information subject hereunder from either the personal information processor or the overseas recipient:

(1) Article 2, except for Articles 2.5, 2.6, 2.7 and 2.11;

(2) Article 3, except for Articles 3.7.2, 3.7.4, 3.9, 3.11, 3.12, 3.13;

(3) Article 4, except for Articles 4.5 and 4.6;

(4) Article 5;

(5) Article 6;

(6) Articles 8.2 and 8.3; and

(7) Article 9.5.

The preceding provisions shall not affect the rights and interests of the personal information subject under the Personal Information Protection Law of the People's Republic of China.

Article 6 Remedies

1. The overseas recipient shall identify a contact person, who is authorised to respond to inquiries or complaints regarding the personal information processing and shall promptly address any inquiries or complaints from the personal information subject. The overseas recipient shall inform the personal information processor of its contact person's information and shall inform the personal information subject of the same in an accessible way by sending a separate notice or publishing an announcement on its website, as below:

Contact person and contact details (phone or email)

2. In case of a dispute between either party hereto and the personal information subject regarding the performance of the Contract, it shall notify the other party and seek cooperation to resolve the dispute.

3. If the dispute cannot be resolved in an amicable way and the personal information subject exercises the rights as a third-party beneficiary pursuant to Article 5, the overseas recipient accepts that the personal information subject protects his or her rights by the following means:

(1) filing a complaint with the regulatory authority; and

(2) filing a lawsuit to the court pursuant to Article 6.5.

4. The parties agree that, when the personal information subject chooses the application of relevant laws and regulations of the People's Republic of China in exercising his or her rights as a third-party beneficiary regarding the dispute hereunder, such choice shall be followed.

5. The parties agree that, if the personal information subject exercises his or her rights as a third-party beneficiary regarding the dispute hereunder, he or she may file a lawsuit to a people's court with jurisdiction in accordance with the Civil Procedure Law of the People's Republic of China.

6. The parties agree that the option made by the personal information subject to protect his or her rights will not undermine the substantive or procedural rights of the personal information subject to seek remedies under other laws and regulations.

Article 7 Termination

1. If the overseas recipient breaches its obligations hereunder, or it is unable to perform the Contract due to any change in personal information protection policies and regulations of the country or region where it is located (including a change in laws or mandatory measures in such country or region), the personal information processor may suspend the transfer of personal information to the overseas recipient until the breach is corrected or the Contract is terminated.

2. If any of the following circumstances occurs, the personal information processor shall have the right to terminate the Contract and notify the regulatory authority if necessary:

(1) Personal information processor has suspended the transfer of personal information to overseas recipients for more than one month pursuant to Article 7.1;

(2) The overseas recipient's compliance with the Contract will violate the laws of the country or region where it is located;

(3) The overseas recipient commits a serious or persistent breach of its obligations hereunder; and

(4) The overseas recipient or the personal information processor has committed a breach of the Contract as determined in a final decision of the competent court or regulatory authority governing the overseas recipient.

In case of Items (1), (2) and (4) above, the overseas recipient may also terminate the Contract.

3. The termination of the Contract by mutual consent of the parties shall not relieve them of their obligations to protect personal information during the personal information processing.

4. Upon termination of the Contract, the overseas recipient shall promptly return or delete the personal information it receives hereunder (including all backups) and shall provide a written explanation to the personal information processor. If it is technically difficult to realise the deletion of personal information, the overseas recipient shall cease any processing apart from storage and necessary safety measures.

Article 8 Liability for breach

1. Each party shall be liable to the other party for any damage caused to the other party due to its breach of the Contract.

2. Either party who violates the rights of the personal information subject as a third-party beneficiary due to a breach hereof shall assume civil liability to the personal information subject, which shall not affect the administrative and criminal liability to be assumed by the personal information processor under the relevant laws and regulations.

3. If the parties are severally and jointly liable, the personal information subject has the right to request either party or both parties to assume liability for compensation. If either party assumes the liability in excess of the proportion to be assumed by it, it has the right to claim compensation from the other party.

Article 9 Miscellaneous

1. In the event of any inconsistency between the Contract and any other legal documents by and between the parties, the terms hereof shall prevail.

2. The conclusion, validity, performance, and interpretation of the Contract, and any dispute arising from the Contract between the parties shall be governed by relevant laws and regulations of the People's Republic of China.

3. All notices given hereunder shall be sent by e-mail, telegram, telex, fax (with confirmation copy sent by airmail) or registered airmail to *(detailed address)* or any other address superseding the aforesaid address as specified in a written notice. If a notice or communication hereunder is sent by registered airmail, it shall be deemed received __ days after the postmark date. If sent by e-mail, telegram, telex, or fax, it shall be deemed received __ business days after it is sent.

4. Any dispute arising from the Contract between the parties and any recovery from the other party by either party for the prior compensation for the damages of personal information subject shall be resolved by the parties through negotiation; if the negotiation fails, either party may adopt the __ of the following means for resolution (if arbitration is chosen, please check the arbitration institution):

(1) Arbitration. The dispute will be submitted to:

- ☐ China International Economic and Trade Arbitration Commission
- ☐ China Maritime Arbitration Commission
- ☐ Beijing Arbitration Commission (Beijing International Arbitration Center)
- ☐ Shanghai International Arbitration Center
- ☐ _____, an arbitral institution of other members of the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards

for arbitration in *(arbitration location)* according to their arbitration rules then in force.

(2) Lawsuit. A lawsuit will be filed to a people's court with jurisdiction in China in accordance with the law.

5. The Contract shall be interpreted in accordance with the provisions of relevant laws and regulations and shall not be interpreted in any manner in conflict with the rights and obligations stipulated in relevant laws and regulations.

6. The original of the Contract is made in __ copies, with each party holding __ copy (copies) and with all copies having the same legal force.

The Contract is signed in *(location)*.

Personal Information Processor:

MM/DD/YYYY

Overseas Recipient:

MM/DD/YYYY

Appendix I

Instructions on Outbound Cross-border Transfer of Personal Information

Details of the outbound cross-border transfer of personal information under the Contract are agreed as follows:

1. Purpose of processing:

2. Method of processing:

3. Scale of personal information to be transferred overseas:

4. Category of personal information to be transferred overseas (please refer to GB/T35273 Information Security Technology - Personal Information Security Specification and relevant standards):

5. Category of sensitive personal information to be transferred overseas (if applicable, please refer to GB/T35273 Information Security Technology - Personal Information Security Specification and relevant standards):

6. The overseas recipient shall only provide personal information to the following third parties outside the territory of the People's Republic of China (if applicable):

7. Transmission method:

8. Overseas storage period: (from MM/DD/YY to MM/DD/YY)

9. Overseas storage location:

10. Other matters (to be specified as appropriate):

Appendix II

Other terms agreed by the parties (if required)

Our Technology, Data Protection and Cybersecurity Practice

We are one of the leading Chinese law firms for Technology, Data Protection and Cybersecurity matters.

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.

All leading international and Chinese legal directories have recognised our abilities, including such as:

CHAMBERS AND PARTNERS

The LEGAL 500

WWL

LEGALBAND

asialaw

CHINA BUSINESS LAW JOURNAL 商法

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

- Data and privacy compliance program
- Privacy policy
- Cross-border data transfers
- 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
- Dispute resolution
- Cyber crimes

This document has been prepared solely for information purposes and is not intended as legal advice.

Visit us at: www.anjielaw.com