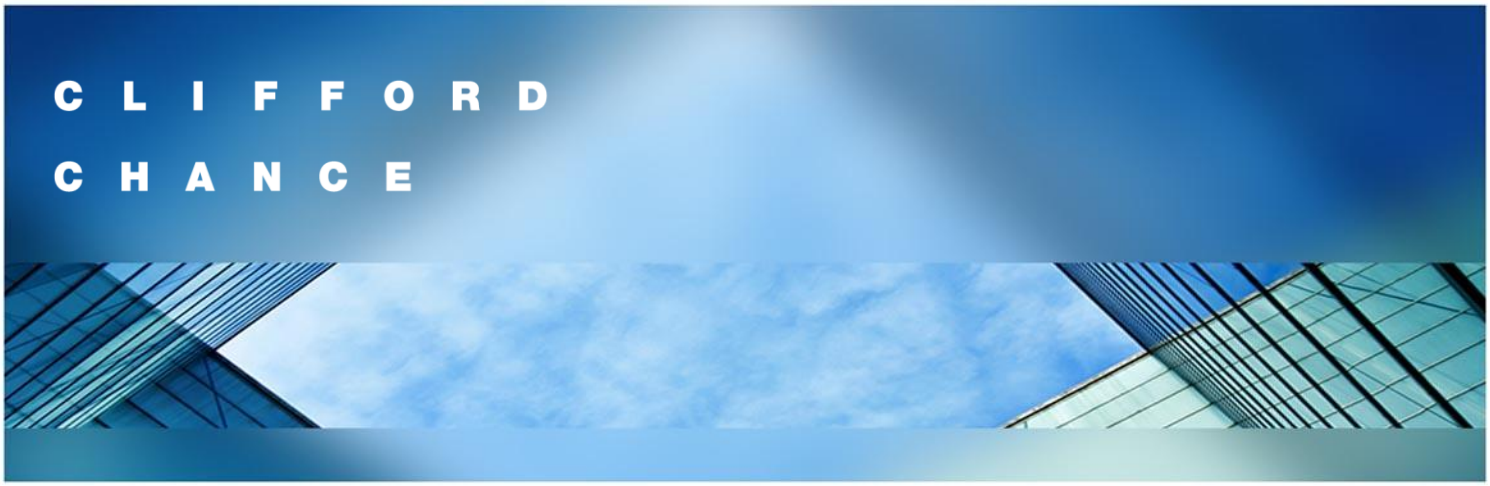


# CHINA FINALISES STANDARD CONTRACT ON CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

In recent years, China[1] has developed its legal framework regulating data and personal information (**PI**) with the promulgation of the *PRC Cybersecurity Law* in 2016, the *PRC Data Security Law* in 2021 and the *PRC Personal Information Protection Law* (the **PIPL**) in 2021 (collectively, the **PRC Data Laws**). The PRC Data Laws set out the supervisory approach of PRC regulators to different data- and PI- related matters. One of the key focuses for multinational companies (**MNCs**) that are subject to the PRC Data Laws is compliance with PRC regulatory requirements on international transfer of PI (*i.e.,* exporting and/or receiving China-sourced PI, including by way of remote access), given the potential widespread implications on their global business and data management systems.

On 24 February 2023, the Cyberspace Administration of China (**CAC**) released the *Measures on Standard Contract for Cross-Border Transfer of Personal Information* (the **SCC Measures**) and the finalised *Standard Contract on Cross-border Transfer of Personal Information* (the **SCCs**), which will take effect on 1 June 2023. The SCC Measures implement the requirements set out under Article 38(3) of the PIPL.

**Key Issues**

- China is continuing its development of its legal framework relating to PI with the introduction of the SCC Measures and the SCCs. These will take effect on 1 June 2023.
- Alongside the security assessment route (measures for which have been recently enacted), the SCCs and the SCC Measures complete the regulatory scheme covering the approved methods for PI export under the PRC Data Laws.
- The SCCs share many common features with the standard contractual clauses under the GDPR, although there are significant differences in the detail.
- Organisations that are subject to the SCC Measures or the SCCs are advised to examine their existing international PI transfer practice in China to ensure compliance by 1 December 2023.
- Organisations receiving China-sourced PI should expect many PI exporters to put in place the SCCs in order to continue cross-border export of such PI, and consider what changes may be required to their data governance processes to allow them to comply with the terms of the SCCs.

## Overview

Under Article 38 of the PIPL, there are three primary channels by which a PI processor can legally transfer PI cross-border. These are:

(a) the security assessment route, as set out under Article 38(1) of the PIPL and further supplemented by the *Security Assessment Measures for Data Export* effective as of 1 September 2022;

(b) the verification route, as set out under Article 38(2) of the PIPL and further supplemented by the *Announcement on Implementation on*

[1] "**PRC**" or "**China**", stands for the People's Republic of China, which for the purpose of this briefing, excludes Hong Kong, Macau or Taiwan.

*Verification and Certification of Personal Information Protection* issued on 4 November 2022; and

(c) the standard contract route, as set out under Article 38(3) of the PIPL and which is now being supplemented by the SCC Measures.

Given the relatively burdensome requirements applicable to the security assessment route (which involves regulatory review and may be time-consuming) and the verification route (which involves third-party inspection of an MNC's data and may trigger confidentiality concerns), it is expected that the standard contract route will be the preferred route for PI export for most MNCs.

However, in order to rely on the standard contract route, MNCs will need to consider whether they can satisfy the applicable threshold conditions discussed below. The European Union has a similar regime under the General Data Protection Regulation (the **GDPR**) and in practice the vast majority of cross border data transfers under the GDPR take place via the standard contract route.

The SCC Measures provide a grace period of six months (until 1 December 2023) for market participants to rectify any potential non-compliance under their existing cross border PI transfer arrangements. Stakeholders including PI processors, overseas recipients and parties that access and process China-sourced PI in business operations exporting or receiving China-sourced PI in the ordinary course of business are advised to prepare for this development and consider taking appropriate measures as soon as possible.

## Key aspects of the SCC Measures

*Applicability of the SCCs*

The SCC Measures provide that a PI processor exporting PI under the SCCs needs to satisfy all of the following conditions:

(1) it is not a critical information infrastructure operator;

(2) it processes the PI of less than 1 million individuals;

(3) it has exported the PI of less than 100,000 individuals since 1 January of the immediately preceding calendar year; and

(4) it has exported sensitive PI of less than 10,000 individuals since 1 January of the immediately preceding calendar year.

If a PI processor does not satisfy any of the above conditions, it will need to rely on other permissible routes for PI export as set out under Article 38 of the PIPL (*i.e.*, the security assessment route or the verification route). In particular, PI processors are not permitted to rely on the SCCs as an alternative to the security assessment route if the threshold for the security assessment has been reached.

*Non-conflict requirement*

The SCC Measures provide that if a PI processor and an overseas recipient have separate agreements on PI export, such agreements must not conflict with the SCCs. The SCCs can be tailored by using Appendix II (*Other Terms Agreed by the Parties (if necessary)*) to the SCCs, which enables the parties to agree on supplemental provisions, provided such provisions are not in conflict with the main body of the SCCs. However, no further guidance has yet been given as to how and to what extent parties can use Appendix II.

While the SCC Measures do not directly regulate an overseas recipient of PI, the SCCs do: (i) impose contractual obligations on an overseas recipient (which include contractually agreeing to accept the supervision of CAC); (ii) explicitly require the SCCs to prevail over any other legal document(s) between the PI processor and the overseas recipient if there is a conflict; and (iii) provide that a data subject is entitled to act as a third-party beneficiary under the SCCs. MNCs receiving China-sourced PI should expect many PI exporters that are subject to the PRC Data Laws to require entry into the SCCs before the expiry of the grace period on 1 December 2023 in order to continue cross-border export of China-sourced PI. Such MNCs should consider (i) what, if any, supplemental provisions they would wish to negotiate and (ii) what changes may be required to their data governance processes to allow them to comply with the terms of the SCCs.

*Key considerations for overseas recipients*

The SCCs set out the rights and obligations of the PI processor and the overseas recipient in relation to PI export at the contractual level. While many of these provisions are similar to the standard contractual clauses under the GDPR (the **GDPR SCCs**), there are notable differences. For example, while the GDPR SCCs include general clauses with a modular approach to cater to four different cross-border data transfer scenarios (*i.e.*, (i) controller to controller; (ii) controller to processor; (iii) processor to controller; and (iv) processor to processor), the SCCs adopt a "one-size-fits-all" approach.

When entering into the SCCs, an overseas recipient will need to carefully consider the following additional issues:

(1) Whether it acts in the capacity of an independent processor (*i.e.*, being able to determine the purpose and the manner of processing – a concept similar to that of 'controller' under the GDPR) or an entrusted processor (*i.e.*, instruction-based processing). Entrusted processors will need to consider the additional obligations provided under the SCCs. These include, for example, providing a written statement on data return and deletion to PI processors when the entrustment agreement with the PI processor is ineffective, invalid or revoked;

(2) Whether it will further delegate processing to a non-PRC sub-processor or transfer the relevant PI to a third party outside China. In that case, the relevant overseas recipient will need to satisfy the additional requirements set out under the SCCs, such as (i) for delegation to a sub-processor, separate consent will need to be obtained by the overseas recipient from the PI processor that exported the PI and overseas recipient will have specific obligations in respect of their supervision over sub-processors; and (ii) for transfers to a third party, making express disclosure to data subjects and making sure that separate/ written consent is obtained from data subjects to cover such onward-transfer. In practice, if there are multiple non-PRC sub-processors, it would be advisable for the relevant overseas recipient to (a) identify the relevant obligations to be passed on to each sub-processor in accordance with the SCCs; (b) carry out a gap analysis between such obligations and their existing agreements; and (c) enter into a supplemental agreement with such sub-processor, if necessary;

(3) The overseas recipient is required to contractually agree to accept the supervision of CAC. It remains to be seen how CAC will exercise such

regulatory oversight in practice. From an enterprise risk perspective, MNCs may consider enhancing the management of China-sourced data through appropriate segregation, tagging and access control measures, as well as keeping proper records. This would be important in the event that an MNC is required to respond to a request from CAC, as the MNC will not then need to spend significant time and effort in identifying China-specific information from comingled group data, noting that providing data protected under laws of other jurisdictions to CAC may trigger other legal implications as well; and

(4) The SCCs provide that a data subject is entitled to act as a third-party beneficiary under the SCCs and can file contractual claims against the PI processor or overseas recipient before a PRC court and/or file an associated complaint with the local provincial Administration of Cyberspace. Notably, the forum for a data subject to file a lawsuit based on the beneficiary right is not affected by the dispute resolution forum that is agreed between the PI processor and the overseas recipient. This means that regardless of what the PI processor and the overseas recipient agree regarding the dispute resolution forum for their respective rights and obligations under the SCCs, a data subject's right to file a claim will not be affected.

*Filing requirement*

PI processors are required to file the executed SCCs together with the PI protection impact assessment report with their local provincial Administration of Cyberspace within 10 business days of the effective date of the executed SCCs. Note that the filing requirement is not a condition precedent for the SCCs to take effect between the PI processor and the overseas recipient, but it enables PRC regulators to monitor the cross border data transfer arrangements.

## What the SCCs mean for Multinational Companies

For MNCs that operate small-to-medium size China offices or branches, it is advisable to analyse the SCCs as part of planning data-related business activities in China. Given the SCC Measures do not provide any exemption from their application, even if an MNC with operations in China does not satisfy the threshold to be subject to a security assessment by CAC, the MNC will nevertheless need to consider and revisit its PI export activities to see whether it needs to enter into the SCCs with its headquarters or other group companies, as well as with any suppliers or other third parties.

In addition to what is agreed with the relevant PI processor under the SCCs, MNCs should note that there are risks of (a) contractual claims from data subjects as discussed above and (b) being inspected or investigated by CAC as a result of any complaint filed by a data subject. The provisions of the SCCs governing cross-border PI transfers (even if only on an intra-group basis) are effectively mandatory under PRC law due to the non-conflict requirement discussed above. The SCCs give data subjects the right to pursue contractual claims as a matter of PRC law before the Chinese courts as beneficiaries under the SCCs against the PI processor and the overseas recipient. This is in addition to the existing rights and remedies under the PIPL and more generally PRC tort law. MNCs should also bear in mind that the PIPL permits public interest lawsuits before the Chinese courts, *i.e.*, proceedings brought by the people's procuratorates, consumer protection organisations and the relevant enforcement agencies specified by CAC for any violations that infringe on the rights and interest of many individuals.

## Outlook

The SCC Measures represent another milestone regulation on PI export in the PRC (*i.e.*, transferring PI to non-PRC country/regions as well as accessing PRC domiciled data from non-PRC country/regions). Given the broad coverage of the SCC Measures, all PI export activities under the SCCs (even where the volume is relatively small) will be required to be disclosed to PRC regulators as a result of the filing requirement under the SCC Measures. While MNCs may have extensive experience with the GDPR compliance regime, it will still be necessary to take a fresh look at the data transfer practices globally in light of the SCC Measures, enhance their intra-group/external contractual arrangements and carefully navigate the challenges of complying with data protection regulatory requirements of multiple jurisdictions.

We have prepared an inhouse translation of the SCCs and are happy to provide this upon request. Please contact us if you wish to discuss and know more about the similarities and/or the differences between the GDPR SCCs and the SCCs.

# CONTACTS

**Ling Ho**
Partner

T + 852 2826 3479
E ling.ho
@cliffordchance.com

**Terry Yang**
Partner

T + 852 2825 8863
E terry.yang
@cliffordchance.com

**Shi Lei**
Partner

T + 86 21 2320 7377
E lei.shi
@cliffordchance.com

**Clarice Yue**
Consultant

T + 852 2825 8956
E clarice.yue
@cliffordchance.com

**Brian Harley**
Consultant

T + 852 2826 2412
E brian.harley
@cliffordchance.com

**Feifei Yu**
Senior Associate

T + 852 2825 8091
E feifei.yu
@cliffordchance.com

**Jane Chen**
Senior Associate

T + 86 10 6535 2216
E jane.chen
@cliffordchance.com

**Sharon Zhang**
Registered Foreign Lawyer

T + 852 2826 3554
E sharon.zhang
@cliffordchance.com

**Jessy Cheng**
Associate

T + 86 10 6535 4935
E jessy.cheng
@cliffordchance.com

Any advice above relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers. This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 33/F, China World Office 1, No. 1 Jianguomenwai Dajie, Chaoyang District, Beijing 100004, People's Republic Of China

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.