UNSW Law & Justice Research Series

China's Standard Contractual Clauses: Restricted Use and Complex Terms

Graham Greenleaf

[2022] *UNSWLRS* 51
(2022) 178 *Privacy Laws & Business International Report*, 1, 6-7

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

China's standard contractual clauses: Restricted use and complex terms

Graham Greenleaf

(2022) 178 *Privacy Laws & Business International Report,* 1, 6-7

At the same time as President Xi Jinping stepped briefly into Hong Kong for his 'victory lap' after dismantling the 'One China, Two Systems' system that it agreed to over 25 years ago, the Cyberspace Administration of China (CAC) issued a consultation draft on 30 June 2022 of its Standard Contract for the Export of Personal Information (SCE), and Provisions governing their use.[1] The consultation finishes on 29 July 2022.

China's SCEs are their equivalent of the EU's SCCs, but are very different in content and when they may be used. In this article, parts of the Provisions are referred to as articles, and parts of the standard contract are referred to as clauses. This article is a short introduction to the SCEs.

Restricted conditions of use

'Personal information handlers' (controllers) must satisfy all four of the following conditions if they wish to use the contract to export personal information (art. 4):

> '(1) Are operators of non-critical information infrastructure;
>
> (2) Handle the personal information of less than 1 million people;
>
> (3) Since January 1 of the previous year, the cumulative amount of personal information provided overseas has not reached 100,000 people;
>
> (4) Since January 1 of the previous year, the cumulative amount of sensitive personal information provided overseas has not reached 10,000 people.'

These restrictive conditions mean that many large-scale information providers based outside China, such as social media platforms, will exceed one of the last three criteria, or are classed as a critical information infrastructure organisation (CIIO), and so will be blocked from SCE use and required to obtain a CAC-conducted security assessment.

Content of each SCE

SCEs must include the following content (art. 6), in addition to the nine standard clauses of the SCE set out in the Appendix to the Provisions:

> '(1) Basic information on the personal information handlers and foreign recipient, including, but not limited to, their name, address, contact persons, and contact information;

[1] Cyberspace Administration of China 'Provisions on Standard Contracts for the Export of Personal Information (Draft for Solicitation of Comments)' 30 June 2020; Source (in Mandarin Chinese) at http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm; English translation by China Law Translate (CLT) at https://www.chinalawtranslate.com/en/ . Quotations in this article are from the CLT unofficial translation.

> (2) The purpose, scope, type, degree of sensitivity, volume, methods, storage period, and storage location for personal information and its exportation;
>
> (3) The responsibilities and obligations of personal information handlers and foreign recipients for protecting personal information, as well as technical and management measures employed to prevent risks that might be brought by the exportation of the personal information, etc.;
>
> (4) The impact of the policies, laws, and regulations of the foreign recipient's nation or region on compliance with the contract provisions;
>
> (5) The rights of the personal information subjects as well as the paths and methods for safeguarding the rights of personal information subjects;
>
> (6) Remedies, contract rescission, liability for breach of contract, dispute resolution, etc.'

It is possible that SCEs may include additional content, given that the final clause of the SCE form is 'Appendix # Other terms agreed upon by both parties', and there is a blank space for additional content. However, any additional content should not contradict or change content already in the SCE.[2]

The nine standard clauses of the SCE set out contractual clauses concerning the following: definitions; warranties by personal information handlers (controllers); obligations of foreign recipients; impact of local laws and policies on these contractual terms; rights of personal information subjects; remedies for breach of contract; rescission of contract; liabilities for damage; applicable law and means of dispute resolution.

Comparison of these SCE clauses with their equivalents in the EU's SCCs is a complex matter but has already been undertaken.[3] Some of the areas of significant difference include: the differing definitions of special/'sensitive' categories, where the PIPL differs significantly from the EU's GDPR; the blanket enforceability of the SCE's data subject rights against both parties to the contract; the SCE's obligations to provide overseas recipients with copies of relevant laws and technical standards, which could involve very expensive translation obligations; different obligations on overseas recipients to demonstrate compliance; the PRC's far more restrictive approach to providing any information to foreign enforcement authorities (which is not resolved in the SCEs, and has uncertain implications); and different periods allowed for data breach notifications.[4]

Requirement and risks of a PIPIA

Before personal information handlers provide personal information abroad, they must first carry out a personal information protection impact assessment (PIPIA), including the following content (art. 5):

> '(1) The legality, propriety, and necessity, of the purposes, scope, and methods of the handling of personal information by the personal information handlers and foreign recipient;
>
> (2) The volume, scope, type, and degree of sensitivity of the personal information exported and the potential risks to the rights and interests in personal information that might be brought;

[2] *Personal Information Protection Act*, art. 38 requires contracts to be 'in compliance with the standard contract provided by the national cyberspace authority'.
[3] Samuel Yang and Chris Fung, AnJie Law Firm 'Cross-border data transfers : A comparison of the EU and Chinese standard contractual clauses' *Lexology,* 8 July 2022
[4] Yang and Fung, ibid

> (3) The responsibilities and obligations that the foreign recipient has pledged to bear, as well as whether the management and technical measures and capacity for the performance of responsibilities and obligations can ensure the security of the exported personal information;
>
> (4) The risk of personal information being leaked, destroyed, altered, abused, and so forth after it is exported, and whether there are clear channels for individuals to preserve rights and interests in personal information, etc.;
>
> (5) The impact of the policies, laws, and regulations of the foreign recipient's nation or region on the performance of a standard contract;
>
> (6) Other matters that might impact the security of exported personal information.'

The controller must file the completed SCE, together with this PIPIA report, with 'the provincial-level internet information department for their area' (the local CAC office) within 10 working days of the SCE taking effect, and they are responsible for its veracity (art. 7).

The controller obviously has the responsibility to 'get it right' when completing a PIPIA, with the risk of very serious consequences, such as cessation of data flows, if they do not, irrespective of what care is taken.

Implementation of the SCE arrangements

Changes to the data or its processing by either contracting party, or changes to the legal environment in either country, during the contractual term must result in another contract being executed and filed with the local CAC equivalent (art. 8).

All parties involved in the contract or its operation, or the filing of contracts and the PIPIA, must preserve confidentiality in relation the information and the contract (art. 9). Organisations and individuals who learn of breaches of the contract have the right to bring a complaint to the provincial level CAC. (art. 10). Where the provincial level CAC learns that there is non-compliance with the management the security of information under the contract, it can order that processing of the information is to cease, including exporting the information (art. 11). If a CAC at provincial level or higher learns of any of the following, it can order cessation of processing (including exporting) and impose criminal or other punishments: (i) failure to follow filing procedures or providing false information; (ii) failure to observe contractual requirements, resulting in harm; or (iii) other circumstances impacting rights and interests.

Conclusions

Although there will be many businesses operating in China who are not eligible to use the Standard Contract for the Export of Personal Information (SCE) because of its restricted conditions of use, for many others the SCEs will make the Personal Information Protection Act (PIPL) far more predictable and usable.