GDR Global Data Review

Comparative analysis of the proposed Chinese standard contract and EU standard contractual clauses

14 December 2022

Rohan Massey, David Chen, Christopher Foo and Pauline Tang.

***Rohan Massey, David Chen**, **Christopher Foo** and **Pauline Tang** of Ropes & Gray analyse and compare key international transfer documents in the EU and Chinese data protection regimes.*

The international transfer of personal data has imposed numerous compliance challenges to international organisations, particularly in the last couple of years due to transfer restrictions arising from local data protection laws.

In 2021, the European Commission updated its set of standard contractual clauses (SCCs) and, combined with the European Court of Justice *Schrems II* ruling, introduced new obligations to assess the risks of personal data transfers and implement appropriate technical and organisational measures.

In June 2022, the Chinese government took steps to implement similar measures first introduced last year in the Personal Information Protection Law (PIPL) through the Regulations on the Standard Contract for Cross-Border Transfer of Personal Information (also known as standard contract regulations), which introduced the draft standard contract for the cross-border transfer of personal data that is subject to PIPL.

Key issues

The Chinese standard contract and the EU SCCs share several conceptual similarities, such as a prior requirement to evaluate the proposed transfer through a transfer impact assessment, a recognition of the principles of transparency (particularly with regards to data subjects) and purpose limitation, as well as an element of commercial flexibility by permitting the addition or annexing of wider commercial agreements as long as they do not contradict protection offered by the SCCs or standard contract.

However, while there are conceptual similarities between the two, there are also key differences. An analysis of these differences reveal several takeaways:

- **Controller-only transfers**: The wording of the Chinese standard contract appears to only contemplate data exports made by data controllers, and does not expressly contemplate transfers made by data processors. On a literal reading this means that organisations in China that process personal data on behalf of data controllers will not be able to make onward transfers out of China, and may require the controllers to enter into a standard contract directly with data importers. This may reduce the effectiveness of data controllers' outsourcing efforts to reduce their data processing burdens.

- **One size may not fit all**: The one-size-fits-all approach adopted by the Chinese standard contract may inappropriately burden foreign data processors in a way that does not suit their designated roles. For example, the Chinese standard contract stops data importers from transferring personal data to third parties located outside of China unless data subjects have been informed of the identity and contact information of the third parties, and separate consent from data subjects has been obtained. However, this responsibility is primarily that of data controllers; data importers that are data processors generally have no way to contact data subjects to provide such notice and obtain such consent, and thus such direct contact with data subjects by data processors is typically inappropriate. In contrast, the EU SCCs allow importers to contact data subjects only when they act as data controllers.
- **Additional regulatory obligations and restrictions**: The Chinese standard contract imposes an additional regulatory obligation on data controllers to file transfer impact assessment reports and the executed contract with provincial cybersecurity regulators. In contrast, SCCs do not require regulatorly involvement as a standard procedure. The Chinese measure is also overall more restrictive than EU SCCs, with the latter containing a larger number of exemptions and grounds to permit the processing of personal data. For example, SCCs permit onward transfers across a wider range of grounds, whereas the Chinese standard contract requires a written agreement to be entered into between data importers and the third-party recipients for all onward transfers. In circumstances where data importers are data processors that rely on a large number of sub-processors for the functioning of their business (such as many SaaS or other cloud-based service providers), it remains to be seen how data controllers relying on the Chinese standard contract for cross-border transfers of personal data out of China can practically comply with this requirement when engaging foreign data processors.
- **Potential conflict with the laws of the importing country**: While not a requirement of the Chinese standard contract, data exporters who are subject to PIPL and the Data Security Law (DSL) are restricted from providing personal data located in China to foreign judicial or law enforcement authorities unless specifically approved by relevant Chinese authorities. In circumstances where data importers are subject to requests for data access (such as a data acquisition order under FISA Section 702 in the US), exporters will need to take steps to comply with such restrictions, potentially resulting in a conflict between importers' legal obligations in connection with such data access requests and contractual obligations they may owe to the data exporters. It remains to be seen how this potential conflict will be addressed in practice.

Detailed comparative analysis of standard contracts and SCCs

	Chinese standard contract	***EU SCCs***
Structure	All clauses apply regardless of the relationship between data exporters and importers, and are intended to be used by a data exporter that is a controller to a data importer that is a controller or processor.	Modular structure with varying clauses that apply depending on whether transfers are: 1. controller-to-controller; 2. controller-to-processor; 3. processor-to-controller; or 4. processor-to-processor.
Scope of application	Data controllers can only enter standard contracts to effect cross-border transfers if: 1. They are not critical information infrastructure operators (ie organisations engaged in important industries or fields, including public communication and information services, energy, transport, water, finance, public services, e-government services, and national defence, and organisations that possess important network facilities, information, or systems that if impaired, damaged, or leaked could result in serious damage to national security, the economy, or public interest);	There are no restrictions on the availability of SCCs.

	2. They process the personal data of less than 1 million individuals; 3. They have transferred the personal data of less than 100,000 individuals in total since 1 January of the preceding year; and 4. They have transferred the sensitive personal data of less than 10,000 individuals in total since 1 January of the preceding year.	
Transfer impact assessments (TIAs)	Prior to any cross-border transfer of personal data out of China, data controllers must carry out TIAs to evaluate: 1. The legality, legitimacy and necessity of the purpose, scope and method of processing; 2. The quantity, scope, type and sensitivity of the personal data to be transferred out of China, and the possible risks to the rights and interests of data subjects; 3. Whether administrative and technical measures undertaken by, and capabilities of, data importers are able to ensure the security of the personal data to be transferred out of China; 4. The risks of unauthorised processing of personal data (including personal data breaches) after it is transferred out of China; 5. Whether data subjects can effectively enforce their rights and interests with regards to their personal data; 6. The impact of the laws and regulations of the country or region where data importers are located; and 7. any other matters that may affect the security of proposed transfers. Data controllers must file reports of the TIA results when they file the standard contracts with the provincial counterparts of the	Data exporters must carry out TIAs before transferring personal data from the EEA to countries that do not benefit from an EU adequacy decision. TIAs should: 1. Identify and assess the risks of the relevant data to be transferred; 2. Identify the relevant data export mechanism to be relied on (ie the SCCs); 3. Assess the data protection laws and practices of the country or region where the data importer is located; and 4. Identify supplementary safeguards to be adopted and re-evaluated periodically, as appropriate to the nature and processing of data. There is no requirement to notify relevant data protection authorities, unless organisations cannot implement any supplementary measures to mitigate the risks identified and still intend to transfer personal data.

	Cyberspace Administration of China where the data controllers are located.	
Onward transfers	Onward transfers may only be performed in the following circumstances: 1. 1. There must be a genuine need to provide personal data for business purposes; 2. Data subjects have been informed of the identity and contact information of third parties who receive the data, the processing purposes and methods, the types of personal data involved, and the methods and procedures to enforce their data subject rights; 3. Consent has been obtained from data subjects (unless consent is not required under Chinese laws and regulations); and 4. The data importers and any third-party recipients have entered a separate written agreement to ensure that recipients will protect the personal data at a level no less than the standard of protection provided by relevant Chinese laws and regulations. Data importers bear joint and several liability with third-party recipients for any harm to data subjects caused by onward transfers.	Onward transfers to third parties are permitted if: 1. Third parties are (or agree to be) bound by obligations as set out in the SCCs between exporters and importers; 2. Transfers are made to a country benefitting from an adequacy decision; 3. Third parties otherwise ensure appropriate safeguards pursuant to articles 46 or 47 of the GDPR; 4. It is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or 5. It is necessary in order to protect the vital interests of the data subject or of another natural person. For controller-to-controller transfers, onward transfers may also be permitted: 6. If third parties enter into written agreements with data importers ensuring the same level of data protection as under the SCCs, and data importers provides a copy of this agreement to data exporters; or 7. If data importers have obtained the explicit consent of data subjects for onward transfers in a specific situation, after having provided them with details of the proposed transfers. Importers must inform exporters and, upon request by exporters, transmit copies of information provided to data subjects.
Regulatory matters	Within 10 business days of the effective date of the standard contracts, data controllers must file executed standard contracts together with a report of TIA results with the	There are no affirmative filing requirements. There is no requirement to enter into new SCCs if there is a change in the circumstances

	provincial counterparts of the Cyberspace Administration of China where controllers are located. New standard contracts need to be concluded if there are any material changes in the processing activities or laws and policies of the destination country since the conclusion of any existing standard contracts. Importers must agree to accept the supervision and administration of, cooperate with and reply to inquiries of, and abide by measures and decisions taken by, the Cyberspace Administration of China and its provincial counterparts.	relating to the data transfer, although the existing SCCs and TIA should be updated accordingly.
Transparency and disclosure	The identity and contact information of all data importers must be disclosed to data subjects. On request, a copy of the standard contracts (which can be redacted to protect trade secrets and other confidential information) must be provided to data subjects together with relevant information about the transfer (including the quantity of personal data transferred).	Data importers must disclose to data subjects: • Their identity and contact information (including a contact point authorised to handle complaints); • The categories of personal data processed; • The right to obtain a copy of the SCCS; and • The purpose of such onward transfers (if applicable) On request, data controllers must make a copy of the SCCs, available to the data subject free of charge. Redactions to protect trade secrets and other confidential information are allowed, but the data controller must provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights, and reasons for redactions must be provided to the best extent possible if data subjects request them.
Data access by foreign authorities	The Chinese standard contract is silent on whether or how the data importer should respond to requests from public authorities located outside of China. However, PIPL and the DSL prohibit organisations subject to the two sets of legislation from providing personal data located in China to foreign judicial or law enforcement authorities, unless otherwise approved by relevant Chinese regulatory authorities..	Where permitted by law, data importers must notify data exporters (and data subjects if possible) when they receive legally binding requests from public authorities, and must only provide the minimum amount of information permissible when responding to such requests.
Governing law and dispute resolution	The Chinese standard contract is governed by Chinese law. Disputes may be resolved by either arbitration by permitted organisations or litigation	The SCCs are governed by the law of an EU member state, with disputes resolved by that member state's courts. For processor-to-controller

	before a people's court with competent jurisdiction in China. Permitted arbitration bodies are: 1. The China International Economic and Trade Arbitration Commission (CIETAC); 2. The China Maritime Arbitration Commission (CMAC); 3. The Beijing Arbitration Commission (Beijing International Arbitration Center); and 4. Other arbitration institutions of member countries of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards.	transfers, SCCs may be governed by, and disputes resolved by the courts of, any country that provides for third-party beneficiary rights.
Permitted alterations	The main body of the standard contract cannot be altered, but parties may supplement it with additional clauses in annex II of each contract. The main body of the standard contract prevails over any inconsistencies between the main body and any additional clauses.	The text of the SCCs cannot be altered, except: 1. 1. To select which module of the SCCs to adopt depending on the role of the data exporter and importer and/or to make specific selections on issues left open in the SCCs (for example, the choice of governing law and dispute resolution forum); 2. To complete the text where necessary, for example to indicate competent courts and regulatory authorities, and to specify certain time periods; 3. To complete annexes; and 4. To include additional safeguards to increase the level of protection of data. Parties may incorporate SCCs into broader commercial contracts, so long as the overall contractual provisions do not contradict with the incorporated SCCs or otherwise prejudice the rights of data subjects.

Next steps

For now, organisations should evaluate their transfers of personal data out of the EEA to assess whether their contractual mechanisms are up to date, and consider assessing their cross-border transfers of personal data out of China, including onward transfers of such data, to determine whether they are able to comply with the Chinese standard contract.

Organisations intending to transfer personal data out of the EEA through the SCCs should ensure their contracts are up to date. Any contracts entered into after 27 September 2021 must incorporate the latest SCCs, and contracts that incorporate the previous form of the EU SCCs should be updated ahead of the European Commission's 27 December 2022 deadline.

Organisations intending to transfer personal data out of China should monitor the development of the Chinese standard contract regulations and updates to the Chinese standard contract while assessing their ability to rely on the Chinese standard contract for such transfers, and what relationships will need to be updated in order address its requirements. In particular, relationships with overseas affiliates and service providers should be examined to determine whether those arrangements can continue in a manner that complies with Chinese cross-border transfer requirements in practice, if these existing arrangements need to be modified, or if new arrangements and service providers need to be put in place.