DATA COMPLIANCE INSIGHTS

Author: YANG, Jianyuan WU, Dan LI, Tianshuo

Latest Updates on China's Mechanisms for Cross-Border Transfer of Personal Information

According to Article 38 of the Personal Information Protection Law ("**PIPL**"), the personal information processor (similar to "data controller" under the GDPR), to provide personal information outside of the People's Republic of China ("**China**", for the sole purpose of this document, not including Hong Kong SAR, Macau SAR and Taiwan Province), shall satisfy any one of the following conditions: (a) pass the security assessment organized by the Cyberspace Administration of China ("**CAC**"), (b) obtain the certification conducted by professional institutes, (c) conclude a standard contract with the overseas recipient, or (d) otherwise provided by laws and regulations.

For the implementation of the above mechanisms for cross-border transfer of personal information under the PIPL, China has issued the *Measures on Security Assessment of Cross-border Transfer of Data (Draft for Comments)* in October 2021, and the *Practice Guide on Cybersecurity Standards – Specifications on Security Certification for Cross-border Processing of Personal Information*, the *Provisions on Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments)* and the *Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments)* in June 2022.

I. Certification for Cross-border Processing of Personal Information

On June 24th, 2022, the Secretariat of the National Information Security Standardization Technical Committee published the Practice Guide on Cybersecurity Standards – Specifications on Security Certification for Cross-border Processing of Personal Information ("Certification Specifications") to implement the certification for personal information protection under the PIPL. The Certification Specifications indicate China's efforts to further explore viable paths for cross-border transfer of personal information, and provides a practical basis for certification bodies to perform certification activities as well as a reference for enterprises to carry out compliance work. Among others, we would like to highlight the following points.

First, the Certification Specifications apply to a specific set of processing activities, namely:

1. The cross-border processing activities within a multinational corporation or among subsidiaries/affiliates of the same economic or utility entity. Moreover, the Certification Specifications require the processor (similar to "controller" under the GDPR) and the overseas recipient to execute a "legally binding and enforceable instrument", including but not limited to a "contract". Such requirement may share some similarities with the Binding Corporate Rules ("**BCRs**") under the GDPR, which is worthy of attention by multinational corporations.

2. The overseas processing activities subject to PIPL's extraterritorial jurisdiction. This involves a quite controversial issue – whether the cross-border rules in Chapter 3 of the PIPL shall apply to the collection of personal information directly from abroad. Possible interpretations include: (a) the initial collection from abroad instantly triggers the cross-border rules, where the overseas processor's specialized agency or designated representative shall act as the domestic processor (similar to "data exporter" under the GDPR); or (b) only the onward transfer triggers the cross-border rules, and the overseas processor may choose the certification as a transfer tool.

Second, the Certification Specifications emphasize repeatedly on the response to regulatory scrutiny and the assumption of legal liabilities.

On the one hand, the domestic entity acts as the regulatory anchor: The Certification Specifications require the domestic company of a multinational corporation or the domestic agency/representative of an overseas processor to apply for the certification and bear the legal liabilities accordingly. Such requirement may raise the concerns of unaffiliated domestic entities (e.g., professional agencies) when considering to represent overseas processors, and thus overseas processors without domestic affiliates may face dilemmas in designating a representative.

On the other hand, both the personal information processor and the overseas recipient shall undertake to comply with the protection level of China's laws and administrative regulations on personal information protection, accept the supervision of China's certification bodies (such as responding to inquiries and routine inspections), and submit to jurisdiction of China's courts.

Third, the Certification Specifications reiterate, specify or even enhance the requirements for cross-border transfer of personal information under the PIPL.

According to the basic requirements of the Certification Specifications, both the personal information processor and the overseas recipient shall designate a person (at decision-making level) in charge of personal information protection (similar to "DPO" under the GDPR) and also a department, execute a legally binding and enforceable instrument ("**Legal Instrument**"), specify the rules for cross-border processing to be observed (including the categories and amounts of personal information, the purposes and manners of processing, the retention periods, the transit areas, the protection of data subjects' rights and interests, the handling of security incidents, etc.). Moreover, the personal information processor shall conduct beforehand an impact assessment on personal information protection ("**PIA**").

In addition, the Certification Specifications emphasize on the protection of data subjects' rights and interests, and extend the scope of exercising such rights (including filing a lawsuit) under the PIPL to overseas recipients. Furthermore, the Certification Specifications specify that data subjects, as the beneficiaries of the terms relating to their rights and interests within the said Legal Instrument, are entitled to obtain a copy of such terms. Such requirement also shares some similarities with the *Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments)*.

II. Standard Contract for Cross-border Transfer of Personal Information

On June 30th, 2022, the CAC issued the Provisions on Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments) ("**Draft Provisions**") and the Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments) ("Draft Standard Contract") to implement the "standard contract" as a transfer tool under the PIPL.

The Draft Standard Contract draws guidance from the Standard Contractual Clauses ("**SCC**") under Article 46.2(c) of the GDPR, and also reflects the China-specific focuses and contexts for personal information protection and supervision. Haiwen has assisted various Chinese companies to implement the EU SCC, especially the substantive safeguards and supplementary measures after the Schrems II case. Companies can refer to the latest regulatory trends reflected in the Draft Provisions and the Draft Standard Contract to prepare for the cross-border transfer in advance, and make corresponding adjustments to the GDPR-based framework (if any). Among others, we would like to highlight the following points.

1. The application scope of standard contract is clarified, and may exclude the companies that transfer abroad a large amount of personal information.

According to the Draft Provisions, the standard contract applies to the personal information processor (similar to "controller" under the GDPR, "**Processor**" or "**Domestic Provider**") who conjunctively meets all the following conditions: the Processor (a) is not qualified as a critical information infrastructure operator; (b) processes the personal information of fewer than 1 million individuals; (c) has not transferred abroad the personal information of more than 100,000 individuals cumulatively since January 1st of the previous year; and (d) has not transferred abroad the sensitive personal information of more than 10,000 individuals cumulatively since January 1st of the previous year.

If contrary to any one of the above conditions, as per the Measures on Security Assessment of Cross-border Transfer of Data (Draft for Comments) ("**Draft Assessment Measures**"), the Processor is required to pass the CAC security assessment as another transfer tool under the PIPL. The Draft Provisions limit the cumulative period to "since January 1st of the previous year" – up to 2 years – and thus somewhat relax the scrutiny for cross-border transfer. However, given China's vast population, the above thresholds of 1 million, 100,000 and 10,000 seem relatively low, and they are set for the Processor as a whole and do not distinguish between business scenarios. Therefore, in practice, many companies may not be qualified to choose the standard contract and instead shall undertake the security assessment.

In addition, standard contract and security assessment share some similarities in practice. For example, the

Draft Assessment Measures require the Processor and the overseas recipient to enter into legally binding instruments such as a contract, and the required terms thereof substantially overlap with the Draft Standard Contract. Since the Draft Standard Contract is formulated by the CAC, companies may refer to its clauses when drafting their contracts for cross-border transfer, even if they cannot leverage the standard contract as the transfer tool.

2. The standard contract requires filing, and thus enables post-hoc supervision.

The Draft Provisions combine the freedom of contract and the supervision by filing. On the one hand, a standard contract takes effect without regulatory approval. On the other hand, the Domestic Provider shall, within 10 working days from the effective date, file to the local, provincial branch of CAC the standard contract (apart from standard terms, also including the case-specific protection measures and factual descriptions) and the PIA report.

Compared with the GDPR, although EU has enhanced the requirement on SCC after the Schrems II case – the data exporter shall prove that personal data is afforded an essentially equivalent level of protection as that of the GDPR, instead of merely signing SCC as a formality – the EU SCC does not require filing.

The filing requirement under the Draft Provisions, albeit not a case-specific approval in security assessment, enables post-hoc supervision by regulatory authorities – the CAC or its provincial branches may notify the Processor in writing to terminate the cross-border transfer if such transfer is found not compliant with regulatory requirements. Where the Processor violates the filing requirements, it may be ordered to rectify within a time limit; where the Processor refuses to rectify or harms the personal information rights and interests, it may be ordered to terminate the cross-border transfer and imposed penalties; where the violation constitutes a crime, the Processor may be held criminally liable.

3. The PIA for cross-border transfer is elaborated on, and the PIA report requires filing.

The PIPL establishes the impact assessment on personal information protection ("**PIA**") and provides for the general items for all applicable scenarios: (a) whether the purposes, manners and other aspects of processing are lawful, legitimate and necessary; (b) the impacts on individuals' rights and interests and the security risks, and (c) whether the protection measures are lawful, effective and proportionate to the risks.

The Draft Provisions further specify the PIA items for cross-border transfer, in particular: (a) the commitments, measures, and capabilities of the overseas recipient to fulfill its obligations and liabilities on personal information protection; (b) the risks of personal information being leaked, destroyed, tampered with, or misused after cross-border transfer; and (c) the impacts on the performance of standard contract by the policies and legislations on personal information protection of the country or region where the overseas recipient is located ("**Overseas Destination**"). The Draft Provisions require the filing of PIA report, but do not specify the granularity of such report, which may become a focus in practice.

While the PIA under the Draft Provisions and the self-assessment on cross-border data transfer under the Draft Assessment Measures share many similarities, the latter additionally emphasizes the assessment of the risks for national security, public interests, and the legitimate rights and interests of individuals and organizations, probably due to the special nature of important data and massive data involved in security assessment.

4. China-version TIA – assessing the impacts on the performance of standard contract by the policies and legislations on personal information protection of the Overseas Destination

The Draft Provisions require the Processor to assess during PIA the impacts on the performance of standard contract by the policies and legislations of the Overseas Destination, and Article 4 of the Draft Standard Contract specifies the items to be assessed. Transfer Impact Assessment ("**TIA**") stems from the additional requirements on EU SCC as a transfer tool after the Schrems II case – to assess whether the laws and practices of the Overseas Destination may prevent the data importer from fulfilling its contractual obligations, and TIA also becomes a part of the latest SCC.

The China version of TIA is simplified from the EU version, but it still seems difficult for many companies. We propose the following considerations for carrying out TIA under the Draft Standard Contract in China, based on our practical experiences of carrying out TIA under the GDPR framework.

Dimension	Requirements under the Draft Standard Contract	Practical Concerns
Formal Element	**Subject of obligation**: TIA is mainly the obligation of the Domestic Provider, but the overseas recipient is obliged to provide necessary information with best efforts and notify the corresponding changes in a timely manner, and both parties shall make warranties and representations and records on TIA.	**Foreign law assessment by a Domestic Provider.** As foreign laws are involved in TIA, it is difficult for a Domestic Provider to prove whether the legal sources are accurate, adequate and up-to-date, whether it has exercised "reasonable diligence", and to coordinate with the overseas recipient and even overseas lawyers.
	Assessment criteria: "Through reasonable efforts", "not knowing" that the policies and legislations on personal information protection of the Overseas Destination will prevent the overseas recipient from performing the standard contract.	
Substantive Element	**Subject of assessment**: The impacts of the policies and legislations on personal information protection of the Overseas Destination on the performance of "this contract", and whether the overseas recipient may be prevented from fulfilling its obligations under "this contract".	**Case-specific assessment or macroscopic assessment.** With a literal interpretation, TIA is case-specific and targeted at this specific transfer and this specific data recipient, rather than a macroscopic assessment targeted at the Overseas Destination as a whole.
	Assessment Ground: in the Overseas Destination: the laws, regulations and standards related to personal information protection, the international organizations joined and the international commitments made, the regulatory and enforcement agencies and judicial bodies, with particular emphasis on the regulatory requirements and previous experience where the public authorities require the overseas recipient to provide or grant access to personal information.	**Assessment on the laws and regulations only, or including the enforcement practices as well**. With a literal interpretation, TIA primarily assesses the laws and regulations on personal information protection, and is limited to the enforcement practices against the overseas recipient.

5. Appropriate technical and organizational measures shall be adopted to effectively safeguard the personal information.

Standard contract is not just paperwork. Instead, the technical and organizational measures agreed upon therein can reduce the security risks in a more direct and effective way, but such measures can be difficult in contract performance and compliance practice. The Draft Standard Contract requires the parties themselves to specify the technical and organizational measures adopted, such as encryption, anonymization, de-identification, and access control. EU has elaborated on such measures in Appendix II of the SCC and EDPB's recommendations

on supplementary measures, which can be references for companies.

Security is not absolute, and the Draft Standard Contract limits the technical and organizational measures to some extent. On the one hand, the Domestic Provider is required to make "reasonable" efforts to ensure that the overseas recipient takes security measures, and the security measures are selected based on the case-specific facts of cross-border transfer. On the other hand, the overseas recipient is required to take "effective" measures, and conduct regular inspections to maintain an "appropriate" level of security. In practice, the scale of security measures will definitely be a key issue but probably without a one-size-fits-all answer.

6. The Onward Transfer of personal information is also regulated, and requires equivalent level of protection guaranteed by written agreement.

The PIPL regulates the "provision to abroad" of personal information by Processor. In addition to the "primary transfer" from China to abroad, the Draft Assessment Measures already notices the "re-transfer" issue after the primary transfer, and the Draft Standard Contract elaborates on the "re-provision" of personal information (i.e., "**Onward Transfer**") in the overseas recipient's obligation.

According to the Draft Standard Contract, the overseas recipient shall not provide personal information to a third party located outside of China unless all of the following requirements are met: (a) there is a genuine business need for Onward Transfer; (b) the data subject is duly informed, and gives a separate consent thereto (unless otherwise provided by laws and regulations); (c) a written agreement is entered into with the third party to ensure its equivalent level of protection, and the overseas recipient assumes joint and several liabilities; and (d) the Domestic Provider is provided with a copy of agreement in (c). Additionally, such third parties shall be specified in Appendix I of the Draft Standard Contract.

China attempts to extend its standards on personal information protection to Onward Transfer through the contractual obligation of the overseas recipient, but there may be difficulties in practice: (a) when entering into a standard contract, the overseas recipient may not accurately anticipate Onward Transfers, especially the identity of third parties (while the EU SCC allows to notify data subjects of the categories of such third parties); (b) the Draft Standard Contract does not specify the granularity of "separate" consent; (c) while an agreement is required, it is not clear whether Onward Transfer may leverage other transfer tools under Article 38 of the PIPL (while the EU SCC allows for multiple transfer tools under the GDPR during Onward Transfer).

7. The application of audit is expanded, and the overseas recipient is obliged to accept audit on the processing activities covered by standard contract.

In the context of personal information protection, "audit" is relatively a new concept and a strong measure to monitor compliance. The PIPL requires the Processor conduct compliance audits on its own processing activities, and the national standard Information Security Technology - Personal Information Security Specification (GB/T 35273-2020) provides for the audits by Processor on its entrusted parties (similar to "processor" under the GDPR) and third-party connected tools (such as SDKs).

The Draft Standard Contract further expands the application of audit, which may become a sticking point in negotiation for the contracting parties. The overseas recipient, either as an independent Processor or entrusted party, is obliged to allow and cooperate with the Domestic Provider to audit the processing activities covered by standard contract, and the Domestic Provider is obliged to provide such audit results to China's regulatory authorities if so required by relevant laws and regulations. In contrast, under the EU SCC, only the processor (similar to "entrusted party" under the PIPL) is obliged to allow for such audits, and no audit is required between two controllers, unless the competent supervisory authority requires an audit on the overseas recipient.

In addition, the Draft Standard Contract provides for two situations in which the overseas recipient is required to provide an audit report to the Domestic Provider: (a) when the contract is terminated, the personal information shall be destroyed or anonymized; and (b) for the entrusted party, when the retention period expires, the personal information shall be deleted or anonymized. In similar cases, the EU SCC only requires the overseas recipient to "certify" such deletion, while the Draft Standard Contract further requires the "provision of an audit report", which also reflects the regulatory authorities' recognition of the form of audit.

8. The individuals are entitled to request a copy of standard contract from both parties, which furthers the right to be informed.

The PIPL stipulates the individuals' right to be informed and requires the Processors to disclose the rules for processing personal information. The Draft Standard Contract further obliges both the Domestic Provider and the

overseas recipient to provide a copy of standard contract upon individual's request. The EU SCC has a similar requirement, but is not yet strictly implemented in practice.

The copy of standard contract is not limited to the standard terms set out by the CAC, but should also include the case-specific protection measures and factual descriptions of the transfer, as is appropriate to protect individuals' right to be informed of their personal information processing. Meanwhile, the Draft Standard Contract also considers companies' needs to protect their trade secrets and other confidential information – the Processor is allowed to reasonably redact such copy, but shall provide a valid summary so that the individuals can understand the contents of contract.

Companies can plan ahead when filling out the standard contract. On the one hand, the Processor can design an appropriate copy of standard contract to balance the individuals' right to be informed and its needs to protect confidential information. On the other hand, the Processor can design a valid mechanism to confirm the identity of individuals and the cross-border transfer involving their personal information, and provide such copy only to the individuals involved in the processing activities under the standard contract to avoid excessive circulation of standard contract.

2022-07-06