MAYER | BROWN

3 March, 2023

Legal Update

China: The "Gold" Standard – Long-Anticipated Standard Contract under Personal Information Protection Law Finalised

The Cyberspace Administration of China ("**CAC**") issued the Measures on Standard Contracts for the Export of Personal Information ("**SC Measures**") on 24 February 2023, finalising the hotly-anticipated standard contract for the export of personal information ("**Standard Contract**") under the Personal Information Protection Law ("**PIPL**"). The SC Measures come after more than a year since PIPL was brought in, and almost eight months after the release of the Draft Provisions on Standard Contracts for the Export of Personal Information ("**Draft Standard Contract Provisions**") (see our previous Legal Update on the Draft Standard Contract).

The finalised Standard Contract becomes effective on 1 June 2023, but with a 6-month grace period (until 30 November 2023) for personal information exports which commenced prior to 1 June 2023.[1] Personal information processors[2] ("**data controllers**") eligible to rely on the Standard Contract (see below section on ***Application***) are expected to revise their data export processes and procedures within the grace period to comply with the SC Measures and the Standard Contract.

Export of Personal Information - Background

Under Article 38 of the PIPL, there are three mechanisms that data controllers may utilise in order to export personal information outside of the People's Republic of China ("**PRC**"): (i) the Security Assessment; ii) the Certification or iii) the Standard Contract.

The Security Assessment was finalised by the CAC last year and took effect on 1 September 2022, while a revised draft Certification specification was recently released on 8 November 2022 and finalised on 16 December 2022 (see our previous Legal Update on the Security Assessment and Revised Certification Specification).

The requirements under the Security Assessment are onerous and mandatory for data controllers that process or export personal information over a certain threshold, or, are deemed to be critical information infrastructure operators ("**CIIOs**"), while the Certification appears to be designed mainly for intra-group transfers.

---

[1] Article 13, SC Measures.

[2] The PIPL uses the term "personal information processor" (not to be confused with the commonly used term "data processor") to refer to "*organizations and individuals that, in personal information processing activities, autonomously decide processing purposes and processing methods*" – this is akin to the concept of a "data controller" under other commonly encountered data protection legislation.

Accordingly, the Standard Contract is likely to be the most widely used mechanism for exporting data out of the PRC. In this legal update, we look at the key provisions of the finalised Standard Contract and the SC Measures.

Application

Under the SC Measures, data controllers must fulfil all the following criteria in order to be able to use Standard Contracts for the export of data. They must be:

1. An entity not classified as a CIIO;
2. Data controllers processing the personal information of less than 1 million data subjects;
3. Data controllers who have exported:
    a. the personal information of **less than** 100,000 data subjects; or
    b. the sensitive personal information of **less than** 10,000 data subjects,

    since January 1 of the previous year; and
4. Also not fall within other circumstances as may be specified by other laws, regulations and rules.

However, the SC Measures now prohibit data controllers from dividing data exports into separate batches to circumvent the Security Assessment.[3] This was previously unaddressed in the Draft Standard Contract Provisions and seemed to be a possible practical solution. The revision ostensibly targets large companies seeking to carry out large data exports through the use of subsidiaries and related companies in a piecemeal fashion, in order to avoid the Security Assessment. Nevertheless, it is unclear in what circumstances a division of personal information would be prohibited and what would be considered *bona fide*.

Obligations of Data Controllers

Under the Standard Contract, data controllers are required to notify data subjects of the foreign recipient's name, contract information, purposes and methods of processing, types and retention period of personal information, the methods and procedures for exercising their rights as a data subject and "*other matters" (see Exhibit 1 (Instructions for the Export of Personal Information*")[4]. Where the export involves sensitive personal information, the necessity and the impact of such export on the rights and interests of the data subjects must also be notified to them.

The primary basis for the collection and processing of personal information under the PIPL is the data subject's consent.[5] However, data controllers are required to obtain separate consent (e.g. unbundled consent) from data subjects in specific scenarios (e.g. export of personal information). The Standard Contract highlights one such scenario where separate, unbundled consent is required for the export of personal information, or from parents or guardians for the export of personal information of minors under the age of 14.[6]

---

[3] Article 4, SC Measures.

[4] Article 2(2), Standard Contract.

[5] Article 13, PIPL.

[6] Article 2(3), Standard Contract.

Notably, data controllers must also inform data subjects of their third party beneficiary rights (see section on *Data Subject Rights* below), which crystalise if the data subject does not expressly object within 30 days.[7]

As the more "proximate" entity to the CAC, data controller exporters have the de facto burden of ensuring that the foreign recipient's data protection practices are sufficient; under the Standard Contract, data controllers have the burden of making "*reasonable efforts to ensure that the foreign recipient will take the necessary technical and management measures (encryption, anonymisation, de-identification, access control, and other technical and management measures)*".[8] Coupled with the added obligations of responding to inquiries from the Regulatory Authority regarding the processing activities of the foreign recipient,[9] and impact assessment to determine whether the foreign recipient's management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported personal information[10], in effect this would mean a full audit of the practices of the foreign recipient pre-transfer. Such documentary evidence in practice will be gathered to satisfy the Personal Information Protection Impact Assessment ("**PIA**") requirements, and will need to be kept for at least 3 years.

Strict Compliance

The SC Measures also now explicitly provide that the Standard Contract is to be used in its entirety, without deviation, unless otherwise directed by the CAC. In any event, while data controllers may include additional clauses in the Standard Contract (as an exhibit), such clauses should not conflict with the Standard Contract, which should prevail in any case.[11] Companies intending to export data out of the PRC should therefore re-visit their pre-existing documentation used for exporting data out of the PRC (e.g. intra-group data transfer agreements, data processing agreements etc.).

PIA

The SC Measures have retained the requirement for data controllers to carry out a PIA prior to the export of personal information. The PIA is to focus on the following areas:

1. The legality, legitimacy, and necessity of the purpose, scope, and methods of personal information processing by the data controller and foreign recipients;
2. The scale, scope, type, and sensitivity of exported personal information, and the potential risks to the rights and interests in personal information that may arise;
3. The responsibilities and obligations undertaken by the foreign recipient, as well as whether the management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported personal information;
4. The risk that personal information will be altered, destroyed, leaked, lost, transferred, or illegally acquired or used during or after export, and whether channels have been

---

[7] Article 2(4), Standard Contract.

[8] Article 2(5), Standard Contract.

[9] Article 2(7), Standard Contract.

[10] Article 2(8)(iii), Standard Contract.

[11] Article 6, SC Measures; Article 9(1), Standard Contract.

established to safeguard data subjects' rights and interests in their personal information rights;

5. The impact of the policies, laws, and regulations of the foreign recipient's jurisdiction on the performance of a standard contract; and
6. Other matters that may affect the security of personal information exported,

and should be kept for at least 3 years.

Data controllers must submit the completed PIA report together with the executed Standard Contract to the regulatory authorities within 10 working days of the effective date of the Standard Contract,[12] though this appears to be a procedural formality without any need for regulatory approval, with data controllers being responsible for the "*veracity of documents filed*".[13]

These requirements are consistent with the PIA requirements under the other Security Assessment and Certification data export mechanisms.

Submission of documents

The SC Measures have retained the requirement for data controllers to submit a new Standard Contract in certain circumstances though the first scenario has been narrowed slightly (dropping changes to the 'quantity' and 'retention period' of personal information). In such an event, the Standard Contract has to be executed again and filed anew with the regulatory authorities:

1. Changes to purpose, scope, type, sensitivity, methods, storage location of exported personal information, and the purposes and methods for which foreign recipients process data, or extend the period of overseas retention of personal information.
2. Changes to the policies, laws or regulations on the protection of personal information in the foreign recipient's jurisdiction that might impact rights and interests in personal information; or
3. Other circumstances that may impact rights and interests in personal information.

However, the SC Measures now allow data controllers to "*supplement [the Standard Contract]*" (i.e. file an addendum) as an alternative to re-filing the entire Standard Contract.

In practice most companies will opt for filing a supplement to the Standard Contract in the event of any of the changes detailed in the first scenario. The second and third scenarios remain tricky given the shifting sands of data protection regulations which will put the onus on data exporters to keep up to date with regulatory and legal changes and make an assessment whether such changes fall within the second scenario. The third scenario is nebulous and difficult to interpret and will likely never be invoked by data exporters but may prove a useful 'stick' for regulators especially if data exports are caught in the cross-fire of geopolitical battles.

The SC Measures now also require data controllers to carry out a new PIA to account for such changes in the scenarios outlined above and file the new PIA alongside the refreshed Standard Contract with the local CAC office. Data controllers should therefore be mindful as to changes to the circumstances in which it exports data since this could require it to prepare and file a new PIA and Standard Contract.

---

[12] Article 7, SC Measures.

[13] Article 8, SC Measures.

Whistleblowing Provision

Violations of the SC Measures can be brought to the attention of the regulators by any third party (e.g. competitors and disgruntled former employees). Companies that export data out of the PRC should be mindful of this provision which highlights again the importance of compliance and of restricting sensitive discussions on data strategy to the C-suite and or personnel in management roles and on a "need to know" basis.

Additional Obligations for foreign recipients

Under the finalised Standard Contract, there are also several new obligations for foreign recipients, including:

1. Obtaining separate consent of data subjects if any personal information is processed beyond the agreed purpose, method of processing and/or type of processing personal information.[14]
2. Obtaining separate consent from parents or other guardians of minors if personal information of a minor under the age of 14 is involved.[15]
3. (For data processor recipients) Returning or deleting personal information if the data processing agreement is ineffective, invalid, revoked or terminated, and providing a written statement to confirm such actions have been taken.[16]

The Draft Standard Contract previously required foreign recipients to take certain actions in the event of a "data breach". This has now been clarified to mean "*the occurrence or possible occurrence of alteration, destruction, leakage, loss, illegally use, unauthorised provision of or access to the processed personal information*".[17]

Under the SC Measures, where there has been a *possible* alteration, destruction, leakage, loss, illegally use, unauthorised provision of or access to the processed personal information, foreign recipients are required to:[18]

1. Take timely remedial action to mitigate adverse effects on data subjects;
2. Immediately notify the data controller and report to the regulatory authority as required by applicable laws, including the types of personal information affected, remedial actions taken, measures data subjects can take to mitigate damage, and the contact details of the personnel responsible for handling the breach; and
3. Document and retain all relevant evidence of alteration, destruction, leakage, loss, illegally use, unauthorised provision of or access including all remedial actions taken.

Laws and regulations of the foreign recipient's jurisdiction

The finalised Standard Contract requires both the foreign recipient and exporting data controller to warrant that they have "*exerted a reasonable duty of care*" when signing the Standard Contract,

---

[14] Article 3(1), SC Measures.

[15] ibid.

[16] Article 3(5), SC Measures.

[17] Article 3(7), SC Measures.

[18] ibid.

and they are not aware of personal information protection laws or regulations of the country where the foreign recipient is located, which include any provisions authorising public authorities to access personal information, that will impact a foreign recipient's performance of their obligations. [19]

This inclusion of "*reasonable duty of care*" is novel to the finalised Standard Contract, and while it is uncertain what this will entail, seems to suggest that a legal opinion of local counsel (of the foreign recipient jurisdiction) may be required – much like the Transfer Impact Assessments required under the GDPR in the wake of Schrems II.

Notably, this is not a blanket restriction on transfers to countries where public authorities may access personal information, but appears to be a point for data controllers to analyse and assess. This is particularly in light of the new Article 4(6) of the Standard Contract, which requires foreign recipients to immediately notify the data controller in the event that it receives a request from a government department or judicial organ of the country in which it is located; data controllers may have to be wary of foreign jurisdictions that allow public authority access and prohibit notifications made to the exporting data controller. The provision mirrors somewhat data controller obligations under the PIPL[20] and Data Security Law ("**DSL**")[21] that prohibit the provision of personal information stored within mainland PRC to judicial or government bodies of foreign countries without the approval of the PRC regulatory authorities.

The Standard Contract allows a data controller to suspend and eventually terminate the contract in the event there are changes in the laws or mandatory measures in the country where the foreign recipient is located which makes it impossible for the foreign recipient to perform the contract. In short, any conflict of laws issue may result in the termination of the Standard Contract.

Data Subject Rights

Other than the data subject rights accorded to data subjects under the PIPL (e,g. access, restriction, correction, withdrawal of consent, portability, erasure etc.), under the finalised Standard Contract, data subjects are granted third party beneficiary rights that allow them to demand performance of various clauses of the Standard Contract[22] and take action for breach of the Standard Contract. In the event of a dispute, the data subject may lodge a complaint with the regulatory authority[23] or file a lawsuit with an appropriate people's court in accordance with the Civil Procedure Law of the PRC for a breach of the Standard Contract by either or both of the parties.[24]

Since such actions (i.e. complaints and/or a civil claim) will necessarily be premised on the information that is made available to the data subject, given the additional rights that data subjects in the PRC have (e.g. third party beneficiary rights[25], right for data subject to obtain a

---

[19] Article 4(1), SC Measures.

[20] Article 41, PIPL.

[21] Article 36, DSL.

[22] Article 5(5), 6(3), Standard Contract.

[23] Article 6(3)(i), Standard Contract.

[24] Article 6(5), Standard Contract.

[25] Article 5(5), Standard Contract.

copy of the SCC from both parties[26], right for data subject to be informed of matters surrounding the export and processing of their personal information [27]), organisations engaged in exporting personal information from the PRC should be mindful of their communications and interactions with data subjects. Data controllers should ensure that they have necessary internal policies and procedures in place to allow them to respond to data subject requests in compliance with the law.

Additional points of interest

The ethos of the Standard Contract appears to be that of discouraging the export of personal information given the requirements for personal information to be exported to "the minimum extent required to achieve the purpose of processing"; or the emphasis on disclosure of the personal information to third parties only if there is a "real business need". This is further driven home by the manner in which the eligibility thresholds for the Standard Contract are framed i.e. "*personal information of less than 100,000 data subjects [counted from 1 Jan of the previous year]*", which point to exports of personal information being the exception rather than the norm since data controllers would have to have meticulous record-keeping practices should they wish to comply with the SC Measures.

Volume thresholds. Data controllers should note that the relevant date for determining whether a data controller falls within threshold 3 (i.e. data controllers who have exported personal information of fewer than 100,000 data subjects or sensitive personal information of fewer than 10,000 data subjects) is January 1 of the *previous year*.[28] Data controllers should therefore be mindful of the volume of personal information they export, particularly in the later part of the year (e.g. December) as this determines whether they are likely to be caught within this threshold, which essentially applies to the export of data for a period of up to 2 years. Where the personal information exceeds the stipulated thresholds in the SC Measures, or the data controller is a CIIO, the Security Assessment transfer mechanism 2 will apply. This will require data controllers to be very precise in their record keeping, and limit data exports on a "need to have" basis should they wish to avoid having to undergo a Security Assessment.

Scope of PIA and Exhibit 1 of the Standard Contract. Since changes to the purpose of processing and/or personal information storage location would necessitate a redo of both the PIA and Standard Contract, data controllers may wish to prepare a more expansive PIA and Exhibit 1 (Instructions on the Export of Personal Information) of the Standard Contract.

Audit Rights. The foreign recipient has a broad obligation to provide the data controller with "all information necessary" to allow it to audit the compliance of processing activities.[29] This is accompanied by a corresponding obligation on the data controller provide all such information (including all compliance audit results) to the CAC as may be required by applicable laws.[30] Accordingly, data controllers engaged in pre-existing data transfers subject to pre-existing agreements should review this documentation to ensure that there are no additional impediments (which may not necessary conflict with the Standard Contract) that may nonetheless impair their ability to comply with the data controller obligations of the Standard Contract.

---

[26] Article 2(9), 3(3), Standard Contract.

[27] Article 2(2), Standard Contract

[28] Article 4, SC Measures.

[29] Article 3(11), Standard Contract.

[3030] Article 2(11), Standard Contract.

Unresolved issues. There are still outstanding questions on the practical applicability of the Standard Contract that remain unanswered e.g when would a division of personal data transfers be considered acceptable? How are data controllers exporting personal information expected to practically keep count of personal information exported, and what happens when a data export crosses the eligibility threshold that would require it to undertake a Security Assessment?

Conclusion

While the finalised Standard Contract sheds more light on the compliance requirements data exporters need to undertake, there are still outstanding practical issues that remain, and businesses with a presence in the PRC and those who deal with companies in the PRC ought to commence preparations to ensure they comply with the SC Measures by 30 November 2023.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrown.com

Joshua Woo
+852 2843 4431
joshua.woo@mayerbrown.com