

Client Alert

PRC Data Protection Updates

27 April 2023

Challenges under China's complex privacy compliance framework

Dora Si and Venus Yim

In recent years, China has intensified its data protection efforts. Apart from the Cybersecurity Law and the Data Security Law, the Personal Information Protection Law (PIPL) also came into force in 2021. This was rapidly followed by a series of implementing regulations and guidelines that fleshed out the substantive requirements.

Heightened requirements under the PIPL

PIPL introduced a more comprehensive but complex legal regime for privacy compliance, applying to the processing of personal information of individuals in the Mainland China, even if the processing activities are conducted *outside Mainland China*.

Informed consent – Apart from the general requirement that personal information should be processed based on the principles of lawfulness, necessity and good faith, the PIPL stipulates that *informed consent* shall be obtained from individuals *before* their personal information is collected, used, or otherwise handled. The exception is where the processing of the personal information is necessary for any of the 5 lawful bases set out in Article 13 of the PIPL:

1. The conclusion or performance of a contract.
2. The performance of statutory responsibilities or obligations.
3. The response to a public health emergency, or the protection of life, health or property of a natural person.
4. News reporting for the public interest and the processing of personal information is within a reasonable scope.
5. Where the personal information disclosed legally in public, or by the individuals themselves, is processed within a reasonable scope.

No regulatory or administrative guidance has been published yet on how these “exceptions to consent” will be implemented. Therefore, it is recommended to seek appropriate consent from individuals.

Separate consent – In certain special circumstances, a “separate”, informed consent will be required including when:-

- sensitive information (such as financial accounts) of an individual is processed;
- personal information is transferred outside Mainland China;
- personal information is provided to, or shared with, another data processor (*including intra-group entities*);
- personal information is made available in public.

Personal information protection officer – A “personal information protection officer” will need to be appointed if the volume of personal information being processed reaches a prescribed threshold, to supervise the processing activities and the implementation of protective technical and organisational measures. Data processors without a local presence, processing personal information outside Mainland China, shall set up special agencies or appoint representatives within the territory to handle relevant data protection matters.

Personal information protection impact assessment – A personal information protection impact assessment (PIA) is a prerequisite for processing sensitive information, using personal information in automated decision-making, providing personal information to another data processor or disclosing the same to the public, and cross-border data transfer.

Cross-border data transfer mechanisms

Apart from fulfilling the consent and PIA requirements, businesses wishing to carry out cross-border transfer of personal information outside Mainland China must also satisfy *at least one* of the conditions:-

	Available mechanism	Criteria/ eligibility
1.	Passing an official security assessment conducted by the Cyberspace Administration of China (CAC)	Mandatory in certain prescribed circumstances: (1) the data processor is a “critical information infrastructure operator”; (2) “important” data is transferred; (3) the personal information of more than 1 million people is being processed; or (4) cumulatively, the personal information of more than 100,000 people, or the sensitive personal information of more than 10,000 people, has been transferred outside Mainland China since 1 January of the preceding year.
2.	Obtaining a personal information security certification	Applicable to cross-border transfer of personal information which does not trigger the application of the official assessment, such as intra-group cross-border transfer of personal information between subsidiaries, or associated companies of multinational companies. The certification applicant should be a PRC legal entity; branches and representative offices do not qualify.
3.	Entering into a contract adopting the Standard Contractual Clauses with the data recipient outside China and recording it with the CAC	Applicable where the compulsory security assessment by the CAC is not triggered.

Official security assessment – The Measures for Security Assessment of Cross-border Data Transfer issued by the CAC (Security Assessment Measures) took effect on 1 September 2022 and set out detailed guidelines. Cross-border data transfer activities to which the Security Assessment Measures apply should have been rectified by the end of February 2023. Those who qualify for official assessment, but failed to do so, are deemed to be in breach of the law but there have been no announcements on the enforcement details yet. In any case, since it is possible to apply for an official assessment anytime, relevant data processors should still apply and not conduct any cross-border transfers without passing the CAC’s assessment.

While the Security Assessment Measures appear to be more relevant to data-heavy businesses with a huge demand for overseas personal information transfer, all data processors are generally recommended to regularly monitor the type and volume of personal information processed. Compliance with the relevant requirements as and when needed will avoid possible disruption to business. Generally, the security assessment results are valid for 2 years, but re-application for assessment is necessary if there is a continued need for cross-border transfer, or there are material changes to the transfer activities.

Personal information security certification – The revised version of the Technical Specification for Certification of Cross-Border Transfers of Personal Information issued on 8 November 2022 clarifies that the certification mechanism applies to all cross-border personal transfers, except where the CAC’s official security assessment mechanism is triggered. The certification is voluntary and, currently, the China Cybersecurity Review Technology and Certification Centre is the only body accredited for certification. Since the certification will only be valid for 3 years once granted, a data processor wishing to continue with cross-border data transfers, should apply for a fresh certification within 6 months before expiry.

Standard contract regime – On 24 February 2023, the CAC issued the long-awaited Measures for the Standard Contract for Cross-Border Transfer of Personal Information (“Measures”), together with the template Standard Contract. The Measures marked the official implementation of the standard contract regime and provides eligible companies with another compliance option; where the data processing activities do not trigger an official assessment, data processors may choose to enter into a contract with the data recipient outside China adopting the standard contract clauses (SCC). Notably, the Measures explicitly prohibit data processors from manipulating the transfers, such as breaking down the amount of personal information processed, to circumvent the CAC security assessment regime.

Under the Measures, the SCC must be adopted but the parties may agree on other contractual terms, provided that they do not contradict the SCC. The SCC extend the obligations under the PIPL to overseas data processors by contractual means, and allows data subjects to exercise rights against the overseas data processors as a third-party beneficiary.

Furthermore, data processors are required to file a copy of the signed contract, together with the PIA report, with the local CAC *within 10 days* from its effective date.

The Measures will take effect from **1 June 2023** with a 6-month grace period for data processors to rectify any non-compliant data transfer. Given that the final deadline for compliance is less than 9 months away, affected companies should take immediate steps to negotiate/ finalize contractual terms, prepare the PIA report and appoint a representative in China for filing the documentations with the CAC.

What's next?

With the implementing rules for all 3 cross-border data transfer mechanisms now in place, increased enforcement actions against non-compliant transfer of personal database outside of China can be expected. Businesses should conduct self-assessments, to identify the nature and volume of personal data involved in cross-border transmissions, and formulate their privacy compliance programs.

Where an official security assessment is not triggered, businesses should consider either voluntary certification or recording a standard contract, to facilitate cross-border transfer activities. Although standard contract recordal has clear advantages in terms of time and cost efficiencies, businesses should review the SCC's compatibility with other data processing obligations applicable to them pursuant to other contractual arrangements or privacy legislation, and harmonize where appropriate.

Want to know more?

Annie Tsoi
Partner

annie.tsoi@deacons.com
+852 2825 9255

Ian Liu
Partner

ian.liu@deacons.com
+852 2826 9630

Catherine Zheng
Partner

catherine.zheng@deacons.com
+852 2825 9617

Tracy Li
Partner

tracy.li@deacons.com
+852 2825 9429

Dora Si
Partner

dora.si@deacons.com
+852 2826 5394

Venus Yim
Associate

venus.yim@deacons.com
+852 2825 5951

The information contained herein is for general guidance only and should not be relied upon as, or treated as a substitute for, specific advice. Deacons accepts no responsibility for any loss which may arise from reliance on any of the information contained in these materials. No representation or warranty, express or implied, is given as to the accuracy, validity, timeliness or completeness of any such information. All proprietary rights in relation to the contents herein are hereby fully reserved.

0427 © Deacons 2023

www.deacons.com