

China proposes to relax cross-border data transfer compliance requirements

Dora Si and Andy Yu

Did you know?

On 28 September 2023, the China Administration of Cyberspace (“CAC”) issued a consultation draft Provision on the Regulation and Promotion of Cross-border Data Transfer (“Draft Provision”) proposing to relax the compliance requirements for cross-border data transfer. The Draft Provision proposes to exempt, under certain circumstances, a data processor’s obligations to either pass an official security assessment, record a standard contract, or obtain a recognised certification (“Transfer Tools”), to facilitate transferring data outside Mainland China as required by Article 38 of the PRC Personal Information Protection Law (“PIPL”).

The circumstances include where the outbound transfer of personal information is necessary:

- (1) for the conclusion / performance of a contract such as the cross-border purchase of goods/services and remittance, booking of air tickets and hotels, visa applications, etc.;
- (2) for human resources management provided that the data processors’ labour rules and regulations and collective contracts are in compliance with the national laws; or
- (3) in an emergency situation for protecting the life, health and property safety of natural persons.

The Draft Provision also clarifies:

- (1) where it is estimated that the outbound transfer involves personal information belonging to *less than* 10,000 data subjects within 1 year, adoption of any Transfer Tool is not required. Notwithstanding this, the consent of data subjects will be required if the outbound transfer is based on consent;
- (2) where it is estimated that the outbound transfer of personal information within 1 year involves *more than* 10,000 but *less than* 1 million data subjects and, provided that either a standard contract concluded with the overseas data recipient has been recorded, or a recognised certification has been obtained, official security assessment is not required. For outbound transfer of personal information of more than 1 million data subjects, official security assessment is required. In any event, the consent of data subjects is required if the outbound transfer is based on consent.

Why does this matter to you?

This is a significant clarification from the CAC concerning the cross-border data transfer security review requirements. It should be encouraging to businesses as the proposed exemptions should lessen the compliance burden on data processors. However, some uncertainties remain.

For instance, as discussed in our previous news alert about the Transfer Tools (see [here](#)), one of the benchmarks triggering official security assessment is where 10,000 or more data subjects’ *sensitive personal information* has been processed since 1 January of the preceding year. It is not clear whether the volume of sensitive personal information processed will remain a determining factor in the Draft Provision’s proposal to exempt data processors from official security assessment.

It is also unclear whether data processors who *process* more than 1 million data subjects’ personal information but actually expect to export less than 10,000 data subjects’ personal information, will be required to adopt any Transfer Tool at all.

How the proposed exemptions will align with other existing or proposed practices needs to be considered. For instance, in the human resources management context, processing of personal information should conform to the labour law requirements. It also remains to be seen how the exemption for transfers necessary for the performance of a contract will be implemented in practice, bearing in mind that it may need to be read together with the new national standard on giving notice and seeking consent in relation to personal information processing effective from 1 December 2023. The necessity of the personal information is a key requirement under the national standard, and this has to be considered in light of the nature of the underlying contracts, as well as the specific purpose of such contracts. This could potentially narrow the application of the contractual exemption under the Draft Provision.

Therefore, in ascertaining their obligations under Article 38 of the PIPL, businesses will need to assess carefully whether their various data processing activities come within the proposed exemptions.

It is important to remember that compliance with Article 38 of the PIPL is not the only obligation applicable to exporting personal information outside Mainland China. Businesses should ensure that their overall practice is in line with the PIPL. For instance, the consent requirement still applies to the extent that consent is relied upon as the legal basis for outbound transfer of personal information, as reiterated in the Draft Provision. Given also the recent release of the draft Measures for Compliance Audit on Personal Information Protection, which proposes to grant more power to the regulators to conduct compliance audit on data processors, businesses should review their practices as soon as possible to manage the increasing data compliance risks.

Want to know more?

Annie Tsoi
Partner
annie.tsoi@deacons.com
+852 2825 9255

Catherine Zheng
Partner
catherine.zheng@deacons.com
+852 2825 9617

Dora Si
Partner
dora.si@deacons.com
+852 2826 5394

Ian Liu
Partner
ian.liu@deacons.com
+852 2826 5360

Tracy Li
Partner
tracy.li@deacons.com
+852 2825 9429

Andy Yu
Senior Associate
andy.yu@deacons.com
+852 2825 9748

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.

1023 © Deacons 2023

www.deacons.com