China – New rules to ease cross-border data transfers: key implications

28 September 2023


The Draft Provisions propose a number of exemptions for businesses which would otherwise be subject to the existing data export restrictions, and will likely have a substantial, but hopefully positive, impact on many international organisations’ on-going China SCC, data export security assessment, and data protection certification projects.

Below are some of the key highlights from our initial review of the Draft Provisions.

What data export activities are exempted from adopting a data transfer mechanism?

Under the Draft Provisions, the following data export activities are exempted having to use one of the three key transfer mechanisms under the PRC Personal Information Protection Law (PIPL):

- **Less than 10k:** Crucially for many B2B operations, where an organisation expects to export personal information of less than 10,000 individuals from the PRC within one year, the transfer mechanisms would not apply. As well as SMEs that struggle to afford to comply with the existing rules, this would ease compliance concerns of many investors, manufacturers and financial institutions which deal solely with commercial and institutional counterparties in mainland China.

- **Contractual necessity:** Exports due to an international services contract, such as for cross-border e-commerce, cross-border payments, plane ticket purchases and hotel bookings, and visa applications will also be exempted. This change, which will be welcomed by retail platforms, leisure and travel players, and financial service institutions, is in line with the exemptions to consent under the PIPL, and a similar contractual necessity exemption under the 2021 draft Regulations on Network Data Security Management.

- **HR management necessity:** Employee data transfers necessary for HR management are exempted in line with the carve-outs from obtaining consent under the PIPL. However:
  - in the absence of an express test as to what amounts to “necessity”, a question remains as to what HR management activities can be outsourced overseas in the manner common to multi-national companies. For example, is relying on a global system for HR management purposes to gain cost efficiencies sufficient? Is it ok to route sensitive salary and bank account details via an overseas system, only to have a local bank be instructed from abroad to execute a domestic remittance?
  - organisations will also need to demonstrate that the HR activities are conducted under their employee handbook or other labour policies. Businesses should
review – if they have not done so – their existing internal practices cover the relevant data export needs.

- **Vital interest**: Data necessary for protecting the health and property safety of a natural person in an emergency may also be transferred without completing one of the mechanisms, which would facilitate international healthcare services, faster disaster and pandemic response, as well as bilateral law enforcement.

- **Non personal information or important data**: If personal information is exported as part of activities relating to international trade, academic cooperation, cross-border manufacturing and production, and marketing activities, this should not trigger the transfer mechanisms. The impact of China’s cross-border transfer restrictions on academic research between universities may be negated, but trials using non-anonymised clinical data would seem still caught.

- **Non-PRC origin personal information**: This carve-out for data entering China from overseas echoes the 2017 draft data export security assessment guidelines, although that draft was never finally released. This may assist the growth of China-based service centres, as were planned in Hainan Free Trade Port in Southern China, and are part of some MNCs’ regional infrastructure.

What does it mean to your ongoing China SCC or security assessment projects?

Following the compliance burden imposed on international businesses through the implementation of security assessments and standard contracts in the last 12 months, the green channels proposed under the Draft Provisions would streamline many multinationals’ data exports, if implemented.

We assume many firms to which exemptions would apply, will halt their China SCC filing or security assessment procedure with the CAC in anticipation of hopefully saving time and costs. However, for applications and filings already lodged with the CAC, there is no express mechanism under the Draft Provisions to withdraw an organisation’s paperwork – often which contains sensitive details on IT infrastructure in China and abroad.

And what about broader compliance programmes?

On the other hand, the exemptions under the Draft Provisions only apply to the data transfer mechanisms under the PIPL, and do not mean that organisations do not need to comply with the general data protection obligations under the PRC’s data laws, including:

- having a **lawful processing basis** such as obtaining consent from data subjects, and separate consent to cross-border data export activities where relying on consent as a basis;
- providing necessary **information notices** specific to the cross-border personal information transfer activities – in particular, the onerous disclosures required under the PIPL about overseas recipients have not been removed; and
- conducting an **impact assessment** (or self-assessment) on the personal information or other regulated data export activities, and documenting the relevant data processing activities. In particular, an assessment of these activities should be a fundament part of organisation’s **accountability records** so as to document its reasons of not adopting a data export mechanism under the PIPL, and its existing and continuous compliance with the PIPL.
In addition, compliance with the newly revised PRC Anti-Espionage Law will be vital in certain information gathering activities (both onshore and offshore) relating to China-based businesses and their activities. Many investment houses, banks and service providers are already – or should be – looking at their data management practices through this lens.

Similarly, organisations must also consider industry-specific obligations. Regulated organisations should particularly focus on assessing their compliance with the data protection requirements under the PIPL and industry rules. For financial institutions, we anticipate data protection and data export compliance will remain a top priority for the financial industry’s regulators, taking the central bank’s draft data security rules as an example.

What’s next?

By emphasising that the central and local cyberspace administrations will “supervise beforehand, during and after the data export activities”, the Draft Provisions emphasise the regulators’ attention on supervising data compliance activities in the PRC.

Overall, the Draft Provisions demonstrate a more favourable outlook for information exchange between China and its trading partners and may ultimately lead to reduced operational and compliance costs for companies operating in or with the world’s second largest economy. The exemptions and green channels provided in the Draft Provisions also echo the recent Greater Bay Area’s data flow initiative and the State Council's Opinions on Boosting Foreign Investment.

The timing for the CAC to finalise the rules is not clear, but we anticipate the regulator will seek to finalise the rules before the 30 November deadline for standard contract filings.

However, as promising as these developments may be, it is essential to recognise that cross-border data transfers remain a multifaceted domain with numerous obligations to meet. There is a pressing need for robust compliance programmes to ensure efficient operations in this data-driven era.

If you are interested in an English translation of the draft provisions, or would like to discuss your data compliance needs, feel free to reach out to us.