# No Longer in Limbo – China's CAC Finalises New Regulations Regarding Cross-border Data Flows

28 March 2024

The much anticipated response to the Consultation initiated by the Cyberspace Administration of China ("**CAC**") last September has finally arrived (read our earlier briefing here). Last Friday, the CAC ended months of speculation by confirming many of the rules initially proposed in the September Consultation, as well as providing additional clarifications by way of the hotly released "Regulations on Promotion and Standardisation of Cross Border Data Flow" ("**Regulations**").

As mentioned, the Regulations provide much-needed clarity on how cross-border data transfers may now be conducted. In this article, we set out our key observations concerning the Regulations and highlight the major developments to the Consultation, in particular, the final exemptions and thresholds regarding an organisation's eligibility to rely on certain cross-border data transfer mechanisms (namely conducting a CAC security assessment, execution and filing of standard contract clauses ("**SCC Filing**"), or certification by CAC-accredited agencies, collectively "**CBDT Requirements**"). A few key observations include:

- **Export of "important data":** Export of "important data" shall be subject to the CAC security assessment at all times. This position remains unchanged from the initial Consultation.
- **Export of overseas personal information:** The Regulations clarify that the CBDT Requirements do not apply to the following scenario: (i) personal information is collected and generated outside Mainland China; (ii) then transferred into Mainland China for processing (without introducing any additional personal information or "important data"); and (iii) then such personal information is subsequently exported to overseas (Art. 4).

- **Exemptions for "genuine need":** Organisations shall be relieved of compliance with the CBDT Requirements where there is a "genuine need" to export the personal information, namely where: (i) the export of personal information is genuinely needed for the conclusion and performance of a contract to which the data subject is a party; (ii) where export of staff's personal information is genuinely needed for an entity's cross-border human resources management implemented in accordance with lawfully established labour rules and regulations and collective bargaining contracts; or (iii) where the export of personal information is genuinely needed for protecting life, health and property safety in emergency situations (Art. 5(1) – (3)).

  In particular, the Regulations now include additional examples of contractual arrangements that may qualify for the exemption, such as cross-border parcel delivery, cross-border payments and cross-border account opening services.

  Importantly, the Regulations also clarify that the exemption may also extend to cross-border human resources management, provided that such cross-border transfer is for a "genuine need". That said, the Regulations have (despite the expectations for further clarity) yet to specify the thresholds

to achieve the “genuine need” or how entities may justify such “genuine need”. Further guidance on this issue is expected.

- **Negative list in free trade zones (“FTZs”):** It remains the case that, for entities registered in FTZs, export of data is exempted from the CBDT Requirements if the data is not set out on the “negative list” for the relevant FTZ (Art. 6).
- **Adjustment of quantitative thresholds for CBDT Requirements:** As many will recall, one of the defining features of the initial Consultation, was the proposed adjustment to certain quantitative “personal information processing thresholds” whereby organisations may be able to benefit from a less-burdensome mechanism to facilitate their cross-border data transfers. Many organisations will be relieved to learn that the flexibility regarding the previously proposed thresholds has been enhanced – specifically the prior 10,000 data subject threshold exemption has been increased to 100,000. For completeness, we have summarised each of the “processing thresholds” below:

| Volume and type of personal information* | Applicable CBDT Requirements |
|---|---|
| **Exporting personal information (without sensitive personal information) of less than 100,000 individuals (Art. 5(4))** | **Exempt from all CBDT Requirements** |
| Exporting personal information (without sensitive personal information) of 100,000 or more but less than 1 million individuals (Art. 8) | SCC Filing or certification by CAC-accredited agencies |
| Exporting sensitive personal information of less than 10,000 individuals (Art. 8) | SCC Filing or certification by CAC-accredited agencies |
| Exporting sensitive personal information of 10,000 or more individuals (Art. 7(2)) | CAC security assessment |
| Exporting personal information (without sensitive personal information) of 1 million or more individuals (Art. 7(2)) | CAC security assessment |
| Exporting any “important data” (Art. 7(2)) | CAC security assessment |

* The volume of personal information shall be calculated on an **annual basis starting from 1 January of the then-current year** (rather than from 1 January of the prior year).

The quantitative processing thresholds do not apply where the data exporter is a “critical information infrastructure operator”, which is still required to conduct CAC security assessments.

Importantly, if organisations are unable to rely on the threshold exemptions summarised above, it is still open for them to consider whether one of the earlier noted “genuine need” or FTZ exemptions may be relied upon.

A helpful inclusion in the Regulations is an extended period of validity of the CAC security assessment, which has been increased from 2 to 3 years from the date on which the assessment result is issued. The 3-year valid period of a result may be extended, subject to the CAC’s approval.

**Other requirements**: The Regulations specifically reiterated the requirement for data exporters to obtain separate consent and undertake privacy impact assessments for exporting personal information. Finally, the Regulations also highlighted that an actual or potential data security incident involving exported data should be remedied and promptly reported to the CAC and other relevant competent authorities.

**Next Steps**

Unsurprisingly, the Regulations are currently in force and have immediate effect. They supersede the existing CBDT Requirements outlined in the Measures on Security Assessment for Export of Data and the Measures on Standard Contract for Export of Personal Information. In light of this, organisations who temporarily paused submission either of the CAC security assessment or filing of the SCCs (pending the CAC’s final confirmation regarding the Consultation – which we now have) are encouraged to revisit their processing activities in light of the clarifications provided and either re-initiate the relevant process or, alternatively, withdraw their application if they are able to rely on the exemptions noted above.

As is often the case, we expect further implementing measures to continue to be published by the CAC and we shall continue to monitor the latest developments.