SQUIRE PATTON BOGGS

China Publishes New Measures and Draft Standard Contract on Data Export

Asia Pacific – 15 July 2022

The past week witnessed two major developments relating to data export from China. Firstly, the data export-related regulation was officially adopted which expands the scope of government assessment. Secondly, the long-awaited draft personal data export standard contract (and the rules relating to the application of this contract) was released for public comment. These related rules require such contracts to be filed with the government.

Measures on Data Export Security Assessment

On 7 July 2022, the Cyberspace Administration of China (the "CAC") released the Measures on Data Export Security Assessment (the "Measures"). These Measures set out the detailed requirements of the security assessment organized by the CAC for data export which is required under the Personal Information Protection Law ("PIPL"), as well as the Data Security Law. Following a draft version in 2021, the Measures clarify the quantities of personal information ("PI") which fall under the PIPL, and add new circumstances that will significantly expand the application of the government's security assessment too.

In particular, bearing in mind the data quantity threshold of 100,000 individuals' PI and 10,000 individuals' sensitive PI, large multinational companies with more than 10,000 employees or customers in China should carefully review whether they would be subject to the government's security assessment.

Threshold for CAC Security Assessment

Data controllers are required to pass the government's security assessment for data export in any of the following circumstances:

1. Export of "**important data**", meaning data that may endanger national security, economic operation, social stability, public health and safety, etc. once it is tampered with, destroyed, leaked, or illegally obtained or used.
2. Export of PI by Critical Information Infrastructure Operators (CIIO). This is in line with the PIPL.
3. Export of PI by a PI controller processing over *1,000,000* individuals' PI (which seems to be the definition of "large volume" PI controller under the PIPL).
4. Cumulative export of PI of more than 100,000 individuals since 1 January of the previous year.
5. Cumulative export of sensitive PI of over 10,000 individuals since 1 January of the previous year, or
6. Other situations as stipulated by the national cybersecurity and informatization department.

Circumstances (4) and (5) are not provided in the PIPL and arguably expand the application of the government's security assessment. It is unclear how the threshold will be calculated. For example, whether any update of PI that is previously exported would be counted within the current year's quota.

CAC Assessment Procedure

Data controllers subject to the assessment should conduct a self-assessment first and submit to the CAC, among other things, the self-assessment report and the data export/process agreements contemplated to be signed with the overseas recipient.

After receiving the completed application documents, the CAC will have six working days to decide whether to accept the application, and another 45 working days to complete the security assessment. This duration may be further extended without a specific time limit. Such indefinite review period has raised concerns of uncertainty that may significantly impact data flow for multinational companies. The result of the security assessment is valid for two years.

Grace Period

The Measures will take effect from 1 September 2022 and offer a six-month grace period for compliance. In other words, data controllers subject to the Measures should make a filing to CAC **before 1 March 2023 at the latest**. Companies in China that are currently exporting critical data or personal data outside of China should take immediate action to assess whether it falls within the scope of the Measures.

Draft PI Export Standard Contract

Also, in relation to the topic of data export, on 30 June 2022, the CAC released the Draft Personal Information Export Standard Contract and the related rules on the application of the standard contract ("Draft Standard Contract") for public comment.

Data controllers that are NOT subject to the government's security assessment as provided under the Measures (as specified above) could rely on the signing of the standard contract to export personal data.

Surprisingly, however, the Draft Standard Contract requires data controllers to file the executed standard contract (and any amendments thereof) to the authorities (CAC) within ten days after it takes effect, together with a PI protection impact assessment report. This is a new requirement not covered by the PIPL. This requirement could significantly increase the burden of data controllers on data export, especially for multinational companies that often have globally centralized management systems. There are also concerns that the filing process may turn into a government review as the CAC may review the filed standard contract and determine whether the data export activities are appropriate.

The Draft Standard Contract sets out detailed requirements on the obligations of the parties in relation to PI protection, and the parties should specify detailed descriptions regarding the export of PI, including (amongst other things) the volume of data and the processing location. The Draft Standard Contract specifically provides that it should prevail over any other agreements between the parties relating to the subject.

The public comment period of the Draft Standard Contract will expire on 29 July 2022. We anticipate that the final version may become available within this year.

Author

Lindsay Zhu
Partner, Shanghai
T: +86 21 61036303
E: lindsay.zhu@squirepb.com

About Us

Our China data privacy team assists regional and multinational companies in dealing with cross-border data protection and transfer, governance and compliance as well as localization. Our clients are from various industries, including high-tech, traditional manufacturing, services, transportation and infrastructure, investment funds, energy and power, telecommunications, and banking and financial services.

They have worked with our regional data team to advise hundreds of clients on various evolving privacy and security requirements.