China Issues Draft Measures on Security Assessment of Cross-border Data Transfer

Monday, November 1, 2021

On October 29, 2021, the Cyberspace Administration of China (“CAC”) released for public comment “Draft Measures on Security Assessment of Cross-border Data Transfer” (“Draft Measures”). The CAC, in its third legislative attempt to build a cross-border data transfer mechanism in China, issued the Draft Measures three days before the November 1, 2021 effective date of the Personal Information Protection Law (“PIPL”).

Scope and Application

If made final, the Draft Measures would apply to cross-border transfers of personal information and “important data” collected and generated in China under certain circumstances.
Data handlers would be subject to mandatory security assessments by the CAC in the following circumstances:

- transfer of personal information and important data collected and generated by critical information infrastructure ("CII") operators (as defined under China's Cybersecurity Law);
- transfer of important data;
- transfer of personal information by data handlers who process over 1 million individuals' personal information;
- cumulatively transferring personal information of more than 100,000 individuals, or "sensitive" personal information of more than 10,000 individuals; or
- other conditions to be specified by the CAC.

The proposed thresholds for triggering such mandatory security assessment generally are lower than what was expected, and likely will impact many international companies.

**Self-Security Assessment**

A data handler subject to a mandatory security assessment would first need to conduct a self-security assessment that addresses the following criteria:

- the legality, propriety and necessity of the proposed cross-border transfer/processing conducted by the data recipient outside of China;
- the volume, scope, type and sensitivity of the data to be transferred, and the potential risks to national security, public interests and the legitimate interests of individual and entities;
- whether relevant management and technical measures implemented by the data exporter and data importer in connection with the transfer will ensure the security of data to be transferred outside of China;
- the risk of data leakage, damage, corruption, loss or misuse, and whether individuals may easily defend their rights; and
- whether the data transfer agreement adequately allocates relevant responsibilities for data protection.

**Mandatory Security Assessment**

Data handlers would need to submit certain materials in connection with a mandatory security assessment, including an application form, the data handler's self-security assessment, and the relevant data transfer agreement. In evaluating a data handler's mandatory security assessment, the CAC would focus on:

- the legality, propriety and necessity of the cross-border transfer;
• the data protection laws and regulations of the data recipient’s jurisdiction, the security of the data being transferred, and whether the protections provided by the data recipient satisfy Chinese laws and regulations and mandatory national standards;

• the volume, scope, type and sensitivity of the data being transferred and the risk of leakage, damage, corruption, loss and misuse;

• whether the data transfer agreement adequately allocates responsibilities for data protection;

• compliance with Chinese laws, administrative regulations and departmental regulations; and

• other matters that are deemed necessary by the CAC.

**Data Transfer Agreement**

The data transfer agreement between the data handler and data recipient would need to include the following content:

• the purpose, method and scope of the cross-border transfer, and the method and purpose of processing by the data recipient;

• the location where the data will be stored outside of China and the data retention period (as well as the measures to be taken upon expiration of the retention period, termination of the data transfer agreement, or otherwise when the purpose of processing has been met);

• provisions restricting re-transfer of the data to other individuals or entities;

• the security measures to be taken in the event of a material change to the data recipient’s business or relevant legal requirements, or if the recipient otherwise cannot ensure the security of the data;

• liability for violations of contractual data security responsibilities, as well as binding and enforceable dispute resolution provisions;

• in the event of a data leak or other breach, provisions requiring the data recipient to respond appropriately and safeguard the rights and interests of individuals’ personal information.

**Procedure of Mandatory Security Assessment**

Upon receipt of the data handler’s application, the CAC would confirm whether it will accept the application within seven business days. After issuing the notice of acceptance, the CAC would have 45 business days to complete the assessment. This period could be extended in complex cases or where the CAC requires supplementary documents, but generally the timeline should not exceed 60 business days.

**Re-Assessment**
The CAC’s mandatory security assessment result would be effective for two years. During this period, the data handler would need to conduct a re-assessment in connection with any of the following conditions:

- changes to the purpose, means, scope and type of the cross-border transfer or processing of personal information and/or important data by the data recipient;
- an extension of the retention period for the personal information and/or important data;
- changes to laws applicable to the data recipient, material changes to the recipient’s business, or amendments to the data transfer agreement that might affect the security of the transferred data; or
- other circumstances that might affect the security of transferred data.

Given that the PIPL is now effective, companies should prepare for the finalization of these Draft Measures and ensure they have plans in place to address compliance with cross-border transfer requirements.

Copyright © 2021, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume XI, Number 305