Articles + Publications | August 9, 2022

Simplifying a Complicated Process — Four Steps to Comply with China's PIPL New Security Assessment Requirements for Cross-Border Data Transfers September 1, 2022

WRITTEN BY

Ronald I. Raether Jr. | Kim Phan | James Koenig | Brent T. Hoard | Joel M. Lutz | Peter T. Wakiyama | Graham T. Dean | Lissette Payne | Robyn W. Lin | Jonathan M. Ishee

Background on the PIPL Security Assessment. On July 7, China's top regulator, the Cyberspace Administration of China (CAC), released the final version of the Measures for Security Assessment of Data Exports (Security Assessment Measures or Measures). Under China's Personal Information Protection Law (PIPL), Article 40, when personal information handlers (the PIPL equivalent of a controller under the GDPR) and critical information infrastructure operators (CIIO) need to export personal information abroad, both handlers and CIIOs must first pass a security assessment organized by the State Cybersecurity and Informatization Department. These Security Assessment Measures will go into effect on September 1, 2022, and existing data export activities must be remediated by March 1, 2023.

Four Steps to Comply with China's PIPL New Security Assessment Requirements: Personal information handlers (*i.e.*, controllers) seeking a security assessment must undertake the following four steps: (1) determine if they meet the threshold, (2) conduct a data protection impact assessment, (3) update any data processing agreements, and (4) submit materials to the CAC, if and as required.

1. Threshold. The Security Assessment Measures apply to personal information handlers and CIIOs that export data overseas. The new guidance sets forth that a security assessment is required when a CIIO or a handler is exporting either important data[1] or personal information, and one of the following applies:

a. The export of any important data;

b. The export of any personal information where the handler processes personal information of more than one million people;

c. The export of personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people, since the previous year; or

d. Any situation provided for by the CAC.

2. Data Privacy Impact Assessment (DPIA). To satisfy the requirement under Article 40 of PIPL to conduct a self-assessment before exporting personal information, an EU-styled Data Protection Impact Assessment (a "DPIA")

could be used as the Chinese PIPL self-assessment is very similar to a DPIA under the GDPR with some additional requirements.

Self-Assessment: Before exporting any data, a business must first perform a self-assessment in accordance with Article 5 of the Measures. This DPIA must focus on the following:

a. The validity, necessity, and appropriateness of the transfer;

b. The scope, category, size, and sensitivity of the data and the impacts that the oversea transfer may have on China's national security, the public interest, or the lawful rights and interests of individual or organizations;

c. Whether the overseas recipient has strong enough organizational and technical measures to protect against any data loss or damage;

d. The risk that data will be tampered with, destroyed, leaked, lost, transferred, or illegally acquired or used during or after export, and whether channels have been established to safeguard data subjects' rights and interest in their personal information rights;

e. Whether the data security protection responsibilities and obligations have been fully stipulated in any data export-related contracts or other legally effective documents formulated with the foreign recipient; and

f. Any other matters that may affect the security of data exported.

Implementation Tip: This self-assessment is essentially a DPIA under the GDPR, with the addition of measures d and e above regarding risk and data security protections.

3. Data Processing Agreements (DPA). Under Article 9 of the Measures, any legal documents, such as the data processing agreement, between the exporter and the overseas recipient, must include several provisions. Many of the requirements are similar to those required under GDPR. However, this DPA provides for more specific remedies, requires the overseas recipient to abide by security measures, and requires specifying measures to be undertaken if data is tampered with. The DPA requirements under Article 9 of PIPL include:

a. The purpose, method, and scope of data exported, and the purpose and method of processing data by oversea recipients;

b. The place and period of data retention abroad, as well as measures to handle exported data after the retention period expires, the agreed purpose is completed, or the legal documents are terminated;

c. Binding requirements for overseas recipients to transfer data to other organizations or individuals;

d. Security measures that the overseas recipient shall adopt when there is a substantial change in its actual control or business scope, or when the data security protection policies, regulations, and network security environment of the country or region where it is located change, or other force majeure circumstances occur that make it difficult to ensure data security;

e. Remedies, liability for breach of contract, and dispute resolution methods for violating data security protection obligations stipulated in legal documents; and

f. When outbound data is tampered with, destroyed, leaked, lost, transferred, or illegally acquired or illegally used, the requirements for properly carrying out emergency response and the ways and means for individuals to safeguard their personal information rights and interests are to be properly carried out.

Implementation Tip: Develop a global form of DPA and update any DPAs to comply with PIPL, the GDPR standard contractual clauses, and the UK's addendum by December 27, 2022 (the deadline for all new and legacy EU SCCs to be updated to the new modules).

4. Submission of Materials. The final packet of materials to be submitted to the CAC includes: (i) the declaration, (ii) the DPIA, (iii) the DPA, and (iv) any other materials required by the CAC. Once materials are submitted, the CAC will have seven working days to decide whether to accept the materials. Once acceptance is complete, the CAC will oversee its own assessment of the data exporting activities, considering many of the same factors considered during the self-assessment. This government assessment will be carried out within 45 business days after application acceptance. A security assessment will be valid for two years; however, new assessments are required in some instances, such as when the business changes the purpose or scope of the overseas data processing activity.

Four Key Steps to Take Prior to September 1, 2022. Since the Measures will go into effect on September 1, 2022, steps for compliance should be undertaken quickly:

1. Conduct a data inventory to determine any export of important or personal information, and if you meet the thresholds established in Article 4 of the Measures.

a. Consider whether these data transfers are necessary and determine whether they can be carried out entirely within China.

b. Pay special attention to the scale of online tracking data collection (*e.g.*, cookies and web beacons) in instances when this data is processed internationally.

2. Conduct data protection impact assessments on existing and future practices. Leverage and expand your EU DPIA to quickly and cost effectively address the PIPL requirements.

3. Consider updating DPAs to incorporate global updates, including those under PIPL, GDPR, and the UK. Although the assessment deadline is September 1, 2022, many companies are using the EU SCC December 27, 2022 deadline as a driver to address global DPA updates.

4. Update internal policies and procedures to ensure these security assessments are conducted in a timely manner. While there has not been much enforcement activity under PIPL, once the security assessment comes into effect September 1, 2022, it will provide a specific action item and filing requirement that the CAC can use in connection with any investigation or regulatory steps it may take. Also keep in mind that for existing data export activities, remediation must be completed by March 1, 2023.

As always, Troutman Pepper's Privacy + Cyber Practice stands ready to assist with global privacy and security compliance, including developing and conducting threshold analysis and security assessments under PIPL, as needed.

Please contact Jim Koenig, Brent Hoard, Kim Phan, or any member of our Privacy + Cyber Practice with questions.

---

[1] Important data is defined in Art. 20 of the Measures, and refers to data that compromises national security, economic operations, social stability, public health, safety, etc.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber